高等院校计算机任务驱动教改教材

网络设备配置与综合实战

张帅　贾如春　主编　　欧洋　张琦　江颖　胡燕　副主编



清华大学出版社

高等院校计算机任务驱动教改教材

网络设备配置与综合实战

张　帅　贾如春　主编
欧　洋　张　琦　江　颖　胡　燕　副主编

清华大学出版社
北　京

内 容 简 介

本书以实际的网络工程为案例，全面深入地介绍了网络设计，网络设备配置与测试，网络安全的规划、配置与实施，网络设备的监控、维护与故障排除等内容。全书紧贴实际应用，将知识介绍和技能训练有机结合起来，融“教、学、做、赛”于一体，突出实用性和可操作性，体现网络技术和网络设备综合实战技能，让读者掌握技能实施必备的理论知识、技术能力要求，以及具备相应的职业素养。全书细化为若干个实践任务，强化学生的实践技能，体现了“项目牵引、任务驱动”和“教、学、做”一体化的思想。本书结合多年国赛、省赛等行业的大赛经验，基于多年项目化教学过程中计算机网络、云计算、大数据专业的课程教学改革成果，并与四川聚比特科技有限公司深度合作，以目前网络运维为技术背景，在参考国内外许多优秀教材的基础上编写而成。

本书适合于不同层次的学生使用，可作为高校计算机相关专业，特别是网络工程、网络运维专业有关课程的教学用书，也可作为网络运维专业技术人员的技术培训资料或工作参考书。

图书在版编目(CIP)数据

网络设备配置与综合实战/张帅，贾如春主编. —北京：清华大学出版社，2018
(高等院校计算机任务驱动教改教材)
ISBN 978-7-302-49387-7

Ⅰ.①网…　Ⅱ.①张…　②贾…　Ⅲ.①网络设备－配置－高等学校－教材　Ⅳ.①TP393

中国版本图书馆 CIP 数据核字(2018)第 014914 号

责任编辑：张龙卿
封面设计：徐日强
责任校对：李　梅
责任印制：董　瑾

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62770175-4278
印 装 者：三河市少明印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**11.25　　**字　　数：**255 千字
版　　次：2018 年 8 月第 1 版　　**印　　次：**2018 年 8 月第1 次印刷
定　　价：35.00 元

产品编号：075737-01

前　言

本书作为计算机网络应用中“网络设备配置”课程的配套教材，十分注重学生实际动手能力方面的培养。本书层次分明，内容图文并茂，实用性较强，既有适度的基础理论知识介绍，又有比较详细的组网实验操作技术讲解。全书根据网络工程师的岗位能力要求和学生的认知规律精心组织教材内容，并围绕一个完整项目展开知识和技能的讲解。交换机和路由器是计算机网络中的核心设备，对于希望今后从事网络系统集成、网络管理与维护等工作的学生，掌握交换机和路由器的基本应用技术十分重要。

本书是计算机网络专业教学资源库建设项目的重要成果之一，也是资源库课程开发成果资源整合应用实践的重要载体。本书编写人员均有多年的项目工程设计、实施和教学经验。本书在设计上满足四个有利的原则：有利于丰富学生的经历，有利于开拓学生的视野，有利于发展学生的个性，有利于学生的自主选择，本书不但反映了学习的过程，还体现了教育的价值。

本书由多年负责企业大数据中心运维工程师及担任计算机网络基础的任课教师共同编写，由川北幼儿师范高等专科学校张帅老师、四川信息职业技术学院贾如春老师担任本书的主编并负责整本书的规划及统稿，由欧洋、张琦、江颖、胡燕一起担任本书的副主编。本书在编写过程中参考了大量书籍和文献，并得到了 H3C 通信技术有限公司的协助，在此一并表示感谢。

本书适合作为高校计算机相关专业，特别是网络工程、网络运维专业有关课程的教学用书，也可作为从事或即将从事网络运维工作的专业技术人员的技术培训用书或工作的参考用书。

由于编写时间仓促，又因为计算机硬件技术发展迅猛，所以书中有不足和疏漏之处在所难免，敬请广大读者批评指正，以便再版时修订，在此表示衷心的感谢。

编　者

2018 年 4 月

目　录

项目 1　VLAN 概 述

1.1　认 识 VLAN

VLAN(Virtual Local Area Network)的中文名称为“虚拟局域网”。虚拟局域网是一组逻辑上的设备和用户,这些设备和用户并不受物理位置的限制,可以根据功能、部门及应用等因素将它们组织起来,相互之间的通信就好像它们在同一网段中一样,由此得名虚拟局域网。VLAN 是一种比较新的技术,工作在 OSI 参考模型的第二层和第三层,一个 VLAN 就是一个广播域,VLAN 之间的通信是通过第三层的路由器来完成的。

1.2　VLAN 的优点与局限性

1. VLAN 的优点

(1) 端口的分隔。即便在同一台交换机上,处于不同 VLAN 的端口也是不能通信的,这样一台物理交换机可以作为多台逻辑的交换机使用。

(2) 网络的安全。不同 VLAN 不能直接通信,杜绝了广播信息的不安全性。

(3) 灵活的管理。更改用户所属的网络不必换端口和连线,只更改软件配置就可以了。

2. VLAN 的局限性

静态 VLAN 虽说是可以使多个端口的设置成一个虚拟局域网,假如两个不同端口、不同虚拟局域网的人员聚到一起协商一些事情,这时候问题就出现了,因为端口及虚拟局域网的不一致往往就会直接导致某一个虚拟局域网的人员不能正常地访问他原先所在的 VLAN(静态虚拟局域网的端口在同一时间只能属于同一个虚拟局域网),这样就需要网络管理人员及时修改该线路上的端口。

对于动态 VLAN,只是在 VLAN 建立初期,网络管理人员需将所有机器的 MAC 进行登记,之后划分出 MAC 所对应的机器的不同权限。

1.3　VLAN 的配置命令

表 1-1 所示是配置 VLAN 时所需用到的一些命令。

表 1-1　VLAN 的配置命令

操作命令	操作说明
system-view	进入系统界面
VLAN number	创建 VLAN,并进入 VLAN 配置界面
port number	将端口加入 VLAN 中
name**	为 VLAN 命名
description**	为 VLAN 进行注释
int VLAN number	进入 VLAN 配置界面

实验　配置 VLAN

实验目的：

- 学会 VLAN 的划分。
- 掌握 VLAN 的命名。

实验设备：H3C-S5820 一台、PC 一台。

VLAN 网络拓扑图如图 1-1 所示。

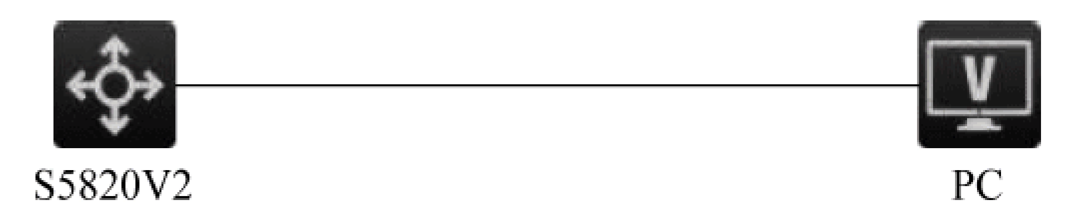


图 1-1　VLAN 网络拓扑图

实验步骤如下：

```
<H3C>system-view                              //进入系统界面
[H3C]vlan 20                                  //创建 VLAN 网
[H3C-vlan20]port GigabitEthernet 1/0/1        //将端口加入 VLAN 20 中
[H3C-vlan20]port GigabitEthernet 1/0/3 to GigabitEthernet 1/0/7
  //将第 3~7 的端口加入 VLAN 20 中
[H3C-vlan20]name IT                           //将 VLAN 命名为 IT
[H3C-vlan20]description 1234567               //注释 VLAN 为 1234567
```

实验结果如下：

```
[H3C]display interface GigabitEthernet 1/0/1 brief Brief
information on interfaces in bridge mode: Link: ADM -
administratively down; Stby - standby

Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface  Link  Speed  Duplex  Type  PVID  Description
GE1/0/1    DOWN  auto    A       A     20   [H3C]display
current-configuration
```

```
interface GigabitEthernet1/0/3 port link-mode bridge
    port access vlan 20
    combo enable copper
#interface GigabitEthernet1/0/4 port link-mode bridge
    port access vlan 20
    combo enable copper
#interface GigabitEthernet1/0/5 port link-mode bridge
    port access vlan 20
    combo enable copper
#interface GigabitEthernet1/0/6 port link-mode bridge
    port access vlan 20
    combo enable copper
#interface GigabitEthernet1/0/7 port link-mode bridge
    port access vlan 20
    combo enable copper
```

项目 2　IP 地址规划

2.1　IP 地址简介

IP 地址是指互联网协议地址（Internet Protocol Address，又译为网际协议地址），是 IP Address 的缩写。IP 地址又称逻辑地址，与 MAC（物理地址）不同，它是由 32 个二进制数组成。每一个网络和每一台计算机都有一个 IP 地址。

2.2　IP 地址的分类

IP 地址由网络号码字段与主机号码字段组成。目前，IP 地址共分为 A、B、C、D、E 五类，比较常用的为 A、B、C 三类。IP 地址分类范围如下。

A 类：0.0.0.0～127.255.255.255

B 类：128.0.0.0～191.255.255.255

C 类：192.0.0.0～223.255.255.255

D 类：224.0.0.0～239.255.255.255

E 类：240.0.0.0～255.255.255.255

2.3　规划 IP 地址的用途

目前，IP 地址属于稀有资源，而 IP 地址规划能使每一台计算机都分配有唯一的 IP 地址，可节省 IP 资源，方便管理计算机网络。另外，也可以在为公司部门划分 VLAN 的同时，依据部门情况而划分 IP 网段。

2.4　IP 地址的配置命令

表 2-1 所示是配置 IP 地址时所需用到的一些命令。

表 2-1　IP 地址的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
int VLAN number	进入 VLAN 配置界面
int number	进入端口配置界面
IP address ×.×.×.× ×.×.×.×	配置 IP 地址
IP address ×.×.×.× ×.×.×.× sub	为同一个端口或 VLAN 配置第二个 IP 地址

实验　IP 地址的规划

实验目的：

- 学会 IP 地址的规划。
- 为 VLAN 规划 IP 网段。

实验设备：H3C S5820 一台、H3C MSR36-20 一台、PC 两台。

1. 用交换机配置 IP 地址

用交换机配置 IP 地址的规划拓扑图如图 2-1 所示。

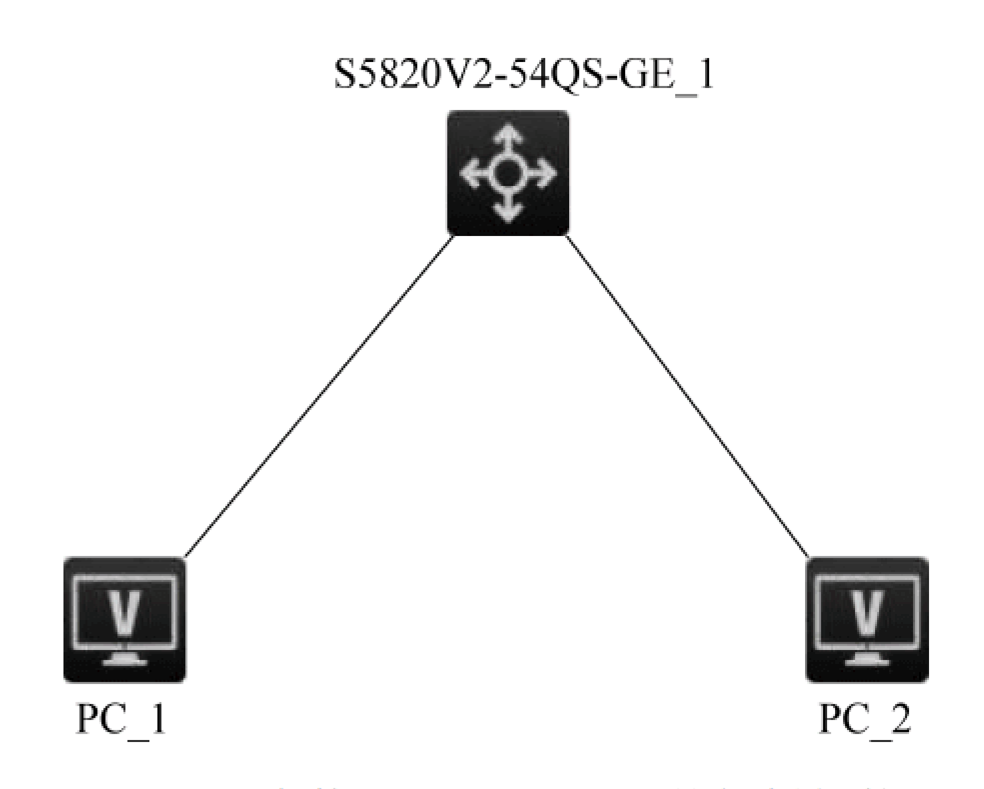


图 2-1　用交换机配置 IP 地址的规划拓扑图

实验步骤如下：

```
<H3C>system-view                                   //进入系统界面
[H3C]vlan 10                                       //创建 VLAN 网
[H3C]interface Vlan-interface 10                   //进入 VLAN
[H3C-Vlan-interface10]ip address 192.16.1.2 24     //设置 IP 地址
[H3C-Vlan-interface10]ip address 192.16.2.2 24 sub //设置第二个 IP 地址
```

实验结果如下：

```
[H3C-Vlan-interface10]display this
#interface Vlan-interface10
```

```
  ip address 192.16.1.2 255.255.255.0
  ip address 192.16.2.2 255.255.255.0 sub
```

2. 用路由器配置 IP 地址

用路由器配置 IP 地址的规划拓扑图如图 2-2 所示。

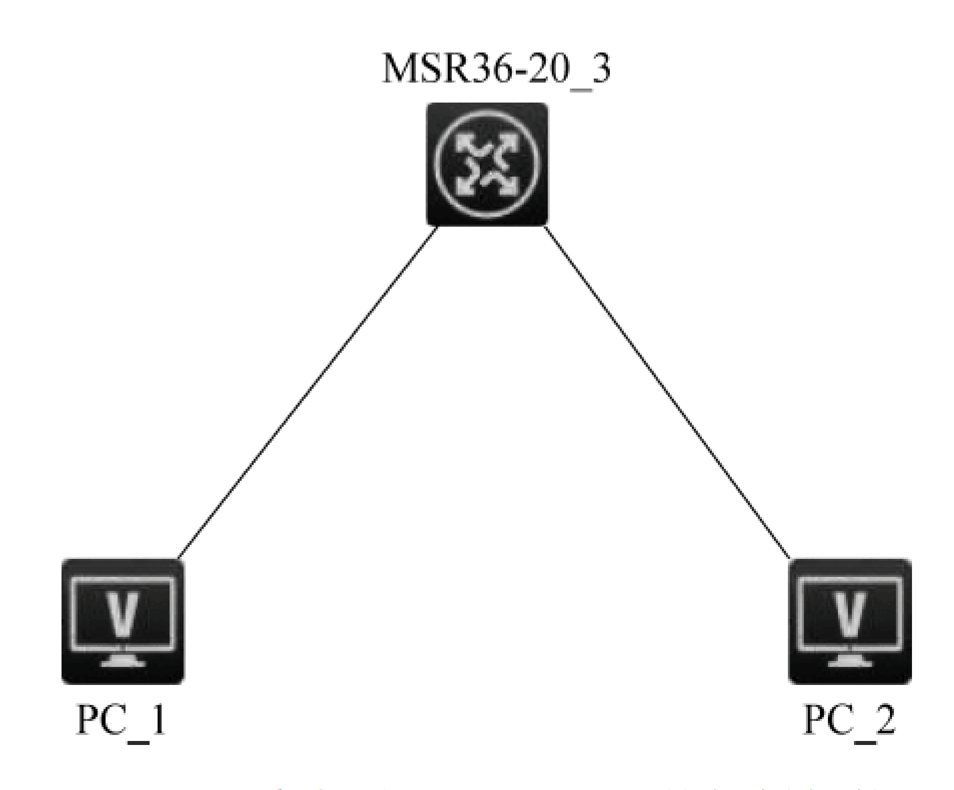


图 2-2　用路由器配置 IP 地址的规划拓扑图

实验步骤如下：

```
<H3C>system-view                                  //进入系统界面
[H3C]hostname Router                              //将路由器命名为 Router
[Router]interface Serial 2/0                      //进入端口
[Router-Serial2/0]ip address 172.16.1.10 24       //设置 IP 地址
[Router]interface Serial 3/0
[Router-Serial3/0]ip address 172.16.2.10 24
```

实验结果如下：

```
[Router]display current-
configuration interface Serial2/0
  ip address 172.16.1.10 255.255.255.0
#interface Serial3/0
  ip address 172.16.2.10 255.255.255.0
#
```

项目 3 局域网部署

3.1 trunk 简 介

trunk 中文名称为“主干线”“中继线”“长途线”。简单地说，端口如果配置为 trunk 模式，则允许多个 VLAN 的数据通过该端口，它为两端设备进行转接，作为信令和终端设备数据的传输链路。

3.1.1 什么情况下使用 trunk

当网络中划分了多个 VLAN 后，为了保证接在不同交换机上的同一 VLAN 中的网络设备能接收和发送多个 VLAN 报文，所以交换机之间互联用的端口必须设置为 trunk，否则相互之间将无法进行通信。

3.1.2 trunk 的配置命令

表 3-1 所示是配置 trunk 时所需用到的一些命令。

表 3-1 trunk 的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
int number	进入端口配置界面
port link-type trunk	设置为 trunk 模式
port trunk permit vlan number	设置允许通过的 VLAN
undo port trunk permit vlan number	关掉已允许通过的 VLAN

实验 1 使 用 trunk

实验目的：掌握交换机端口 trunk 的配置，使多个 VLAN 相互通信。

实验设备：H3C S5820 三台。

交换机 trunk 端口配置拓扑图如图 3-1 所示。

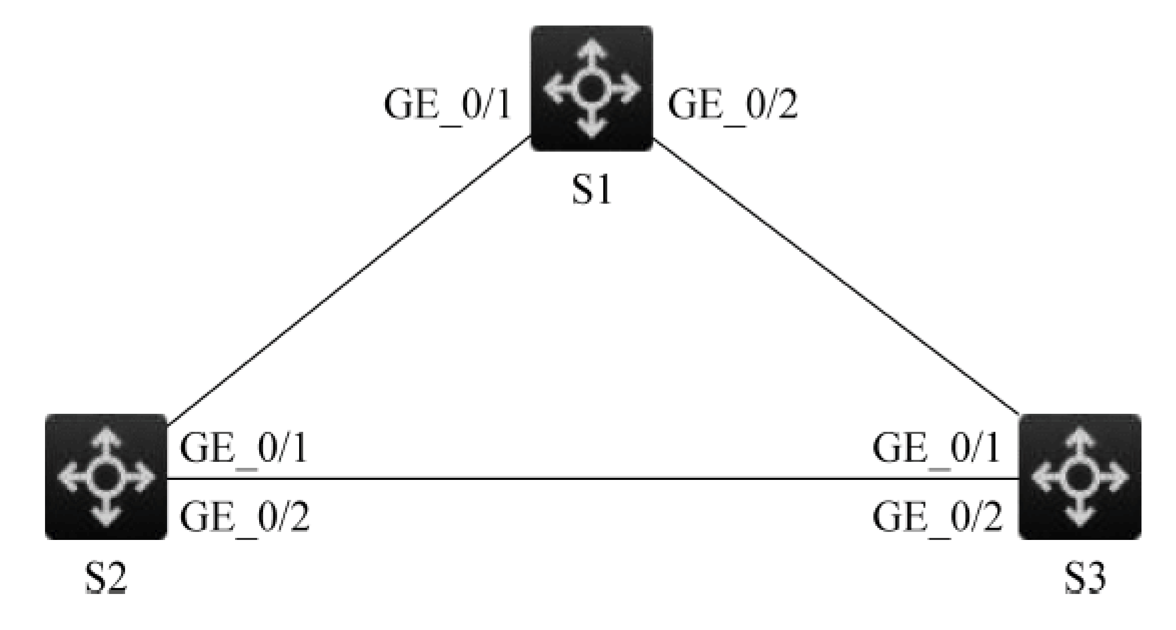


图 3-1　交换机端口 trunk 配置拓扑图

实验步骤如下：

```
[S1]vlan 10
[S1-vlan10]vlan 20
[S1-vlan20]vlan 30
[S1-vlan30]vlan 40
[S1-vlan40]vlan 50
[S1-vlan50]quit
[S1]interface GigabitEthernet 1/0/1                //进入端口 1
[S1-GigabitEthernet1/0/1]port link-type trunk      //将端口设置为 trunk 模式
[S1-GigabitEthernet1/0/1]port trunk permit vlan 10 20 30 40 50
  //允许 VLAN 10~VLAN 50 的整十数据通过
[S1-GigabitEthernet1/0/1]undo port trunk permit vlan 1
  //关闭 VLAN 1,让不必要的 VLAN 数据不通过
[S1]interface GigabitEthernet 1/0/2
[S1-GigabitEthernet1/0/1]port link-type trunk
[S1-GigabitEthernet1/0/1]port trunk permit vlan 10 20 30 40 50
[S1-GigabitEthernet1/0/1]undo port trunk permit vlan 1
[S2]vlan 10
[S2-vlan10]vlan 20
[S2-vlan20]vlan 30
[S2-vlan30]vlan 40
[S2-vlan40]vlan 50
[S2-vlan50]quit
[S2]interfaceGigabitEthernet1/0/1
[S2-GigabitEthernet1/0/1]portlink-typetrunk
[S2GigabitEthernet1/0/1]port trunk permt vlan10 20 30 40 50
[S2-GigabitEthernet1/0/1]undo port trunk permit vlan 1
[S2]interface GigabitEthernet 1/0/2
[S2-GigabitEthernet1/0/1]port link-type trunk
[S2-GigabitEthernet1/0/1]port trunk permit vlan 10 20 30 40 50
[S2-GigabitEthernet1/0/1]undo port trunk permit vlan 1

[S3]vlan 10
[S3-vlan10]vlan 20
[S3-vlan20]vlan 30
```

```
[S3-vlan30]vlan 40
[S3-vlan40]vlan 50
[S3-vlan50]quit
[S3]interfaceGigabitEthernet1/0/1
[S3-GigabitEthernet1/0/1]port link-type trunk
[S3-GigabitEthernet1/0/1]port trunk permit vlan 10 20 30 40 50
[S3-GigabitEthernet1/0/1]undo port trunk permit vlan 1
[S3]interface GigabitEthernet 1/0/2
[S3-GigabitEthernet1/0/1]port link-type trunk
[S3-GigabitEthernet1/0/1]port trunk permit vlan 10 20 30 40 50
[S3-GigabitEthernet1/0/1]undo port trunk permit vlan 1
```

实验结果如下：

```
[S1]display current-configuration
interface GigabitEthernet1/0/1 port
link-mode bridge
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 10 20 30 40 50
  combo enable copper
# interface GigabitEthernet1/0/2 port link-mode bridge
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 10 20 30 40 50
  combo enable copper
#
[S2]display current-configuration
interface GigabitEthernet1/0/1 port
link-mode bridge
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 10 20 30 40 50
  combo enable copper
# interface GigabitEthernet1/0/2 port link-mode bridge
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 10 20 30 40 50
  combo enable copper
#
[S3]display current-configuration
interface GigabitEthernet1/0/1 port
link-mode bridge
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 10 20 30 40 50
  combo enable copper
# interface GigabitEthernet1/0/2 port link-mode bridge
  port link-type trunk
```

```
  undo port trunk permit vlan 1
  port trunk permit vlan 10 20 30 40 50
  combo enable copper
#
```

3.2 生成树协议

生成树协议(STP,Spanning Tree Protocol)主要是为了防止二层网络(交换机或网桥)产生网络环路,避免因环路的存在而造成广播风暴问题。

3.2.1 STP 的操作原理

1) 选择根网桥

选择根网桥的依据是网桥 ID,由优先级和 MAC 地址组成。先看优先级,优先级相同时再看 MAC 地址,值越小越优先选择。

2) 选择根端口

每一个非根网桥将从其接口选出一个到根网桥管理成本(administrative cost)最低的接口作为根端口,选择的依据:①自身到达根网桥的根路径是成本最低的接口;②直连网桥 ID 最小;③端口 ID 最小。

3) 选择指定端口

当一个网段中有多个网桥时,这些网桥会将它们到根网桥的管理成本都通告出去,其中具有最低管理成本的网桥将作为指定(designated)网桥。指定网桥中发送最低管理成本的 BPDU 的接口是该网段中的指定端口。在每段链路上,选择一个指定端口,选择的依据如下。

(1) 发送最低根路径成本的 BPDU 的接口;

(2) 所在网桥 ID 最小;

(3) 端口 ID 最小。

3.2.2 STP 的端口状态

STP 的端口状态有以下几种。

(1) 学习:交换机端口监听 BPDU,并学习此交换式网络中的所有路径,但不转发数据包。

(2) 监听:该端口正在等待接收 BPDU 数据包,BPDU 可能告知该端口重新回到阻塞状态。

(3) 阻塞:被阻塞的端口不能对数据帧进行转发,只监听 BPDU 帧。

(4) 转发:它会转发帧,也会发送和接收 BPDU 帧。

(5) 禁用:该第二层端口不参与生成树,不会转发帧。禁用状态下的端口是不工作的。

```
  undo port trunk permit vlan 1
  port trunk permit vlan 10 20 30 40 50
  combo enable copper
#
```

3.2 生成树协议

生成树协议(STP,Spanning Tree Protocol)主要是为了防止二层网络(交换机或网桥)产生网络环路,避免因环路的存在而造成广播风暴问题。

3.2.1 STP 的操作原理

1) 选择根网桥

选择根网桥的依据是网桥 ID,由优先级和 MAC 地址组成。先看优先级,优先级相同时再看 MAC 地址,值越小越优先选择。

2) 选择根端口

每一个非根网桥将从其接口选出一个到根网桥管理成本(administrative cost)最低的接口作为根端口,选择的依据:①自身到达根网桥的根路径是成本最低的接口;②直连网桥 ID 最小;③端口 ID 最小。

3) 选择指定端口

当一个网段中有多个网桥时,这些网桥会将它们到根网桥的管理成本都通告出去,其中具有最低管理成本的网桥将作为指定(designated)网桥。指定网桥中发送最低管理成本的 BPDU 的接口是该网段中的指定端口。在每段链路上,选择一个指定端口,选择的依据如下。

(1) 发送最低根路径成本的 BPDU 的接口;

(2) 所在网桥 ID 最小;

(3) 端口 ID 最小。

3.2.2 STP 的端口状态

STP 的端口状态有以下几种。

(1) 学习:交换机端口监听 BPDU,并学习此交换式网络中的所有路径,但不转发数据包。

(2) 监听:该端口正在等待接收 BPDU 数据包,BPDU 可能告知该端口重新回到阻塞状态。

(3) 阻塞:被阻塞的端口不能对数据帧进行转发,只监听 BPDU 帧。

(4) 转发:它会转发帧,也会发送和接收 BPDU 帧。

(5) 禁用:该第二层端口不参与生成树,不会转发帧。禁用状态下的端口是不工作的。

3.2.3　RSTP 简介

RSTP 由 IEEE 制定的 802.1w 标准定义，它在 STP 基础上进行了改进，实现了网络拓扑的快速收敛。其“快速”体现在：当一个端口被选为根端口和指定端口后，其进入转发状态的延时在某种条件下大大缩短，从而缩短了网络最终达到拓扑稳定所需要的时间。

3.2.4　MSTP 原理

MSTP 将整个二层网络划分为多个 MST 域，各个域之间通过计算生成 CST；域内则通过计算生成多棵生成树，每棵生成树都被称为是一个多生成树实例。其中，实例 0 被称为 IST，其他多生成树实例为 MSTI。MSTP 同 STP 一样，使用配置消息进行生成树的计算，只是配置消息中携带的是设备上 MSTP 的配置信息。

3.2.5　STP 的配置命令

表 3-2 所示是配置 STP 时所需用到的一些命令。

表 3-2　STP 的配置命令

操作命令	操作说明
system-view	进入系统界面
stp region-configuration	进入 MSTP 配置界面
region-name name	为 MSTP 配置域名
instance id vlan number	配置 VLAN 映射表
revision-level	配置 MSTP 的修订级别
active region-configuration	激活 MSTP 域
stp instanceid root primary	设置实例为主根
stp instanceid root secondary	设置实例为从根

实验 2　配置 MSTP

实验目的：掌握 MSTP 的配置，学会如何防止二层网络产生网络环路。

实验器材：H3C S5820 三台。

实验要求：region-name 为 H3C。

实例 1 对应 VLAN 10、VLAN 20，实例 2 对应 VLAN 30、VLAN 40。

S1 作为实例 1 中的主根，以及实例 2 中的从根；S2 作为实例 2 中的主根，以及实例 1 中的从根。

MSTP 的配置拓扑图如图 3-2 所示。

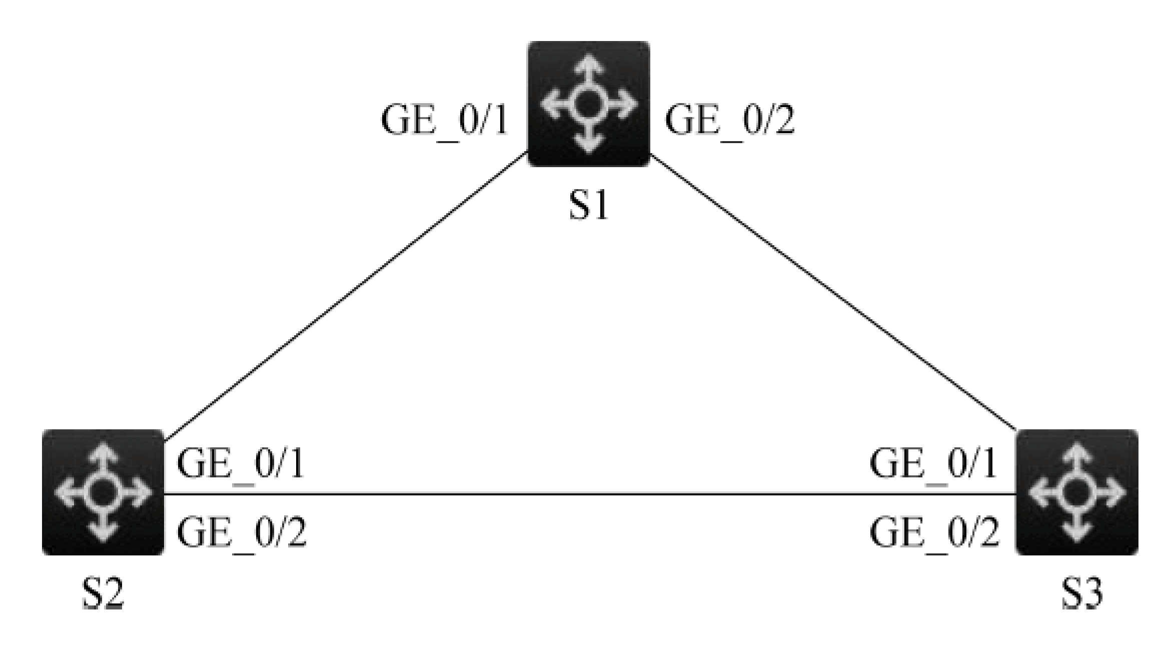


图 3-2　MSTP 的配置拓扑图

实验步骤如下：

```
[S1]vlan 10
[S1-vlan10]vlan 20
[S1-vlan20]vlan 30
[S1-vlan30]vlan 40
[S1-vlan40]quit
[S1]interface GigabitEthernet 1/0/1
[S1-GigabitEthernet1/0/1]port link-type trunk
[S1-GigabitEthernet1/0/1]port trunk permit vlan 10 20 30 40
[S1]stp region-configuration            //进入 MSTP 域视图
[S1-mst-region]region-name H3C          //配置 MSTP 域的域名为 H3C
[S1-mst-region]instance 1 vlan 10 20    //将 VLAN 10、VLAN 20 映射到生成树实例 1 上
[S1-mst-region]instance 2 vlan 30 40    //将 VLAN 30、VLAN 40 映射到生成树实例 2 上
[S1-mst-region]active region-configuration     //激活 MSTP 域
[S1-mst-region]quit
[S1]stp instance 1 root primary         //设置实例 1 为主根
[S1]stp instance 2 root secondary       //设置实例 2 为从根
[S2]vlan 10
[S2-vlan10]vlan 20
[S2-vlan20]vlan 30
[S2-vlan30]vlan 40
[S2-vlan40]quit
[S2]interface GigabitEthernet 1/0/1
[S2-GigabitEthernet1/0/1]port link-type trunk
[S2-GigabitEthernet1/0/1]port trunk permit vlan 10 20 30 40
[S2]stp region-configuration
[S2-mst-region]region-name H3C
[S2-mst-region]instance 1 vlan 10 20
[S2-mst-region]instance 2 vlan 30 40
[S2-mst-region]active region-configuration
[S2-mst-region]quit
```

```
[S2]stp instance 1 root secondary        //设置实例 1 为从根
[S2]stp instance 2 root primary          //设置实例 2 为主根
```

实验结果如下：

```
[S1]display stp brief
MST  ID  Port                  Role  STP State   Protection
0        GigabitEthernet1/0/1  DESI  FORWARDING  NONE
0        GigabitEthernet1/0/2  DESI  FORWARDING  NONE
1        GigabitEthernet1/0/1  DESI  FORWARDING  NONE
2        GigabitEthernet1/0/1  ROOT  FORWARDING  NONE

[S2]display stp brief
MST  ID  Port                  Role  STP State   Protection
0        GigabitEthernet1/0/1  ROOT  FORWARDING  NONE
0        GigabitEthernet1/0/2  DESI  FORWARDING  NONE
1        GigabitEthernet1/0/1  ROOT  FORWARDING  NONE
2        GigabitEthernet1/0/1  DESI  FORWARDING  NONE
```

3.3 VRRP 简 介

VRRP 是 Virtual Router Redundancy Protocol 的缩写，译为虚拟路由冗余协议，是一种容错协议。它通过把几台路由设备联合组成一台虚拟的路由设备，并通过一定的机制来保证当主机的下一跳设备出现故障时，可以及时将业务切换到其他设备，从而保持通信的连续性和可靠性。主要是解决局域网主机访问外部网络的问题。VRRP 包括 VRRPv2 和 VRRPv3 两个版本，VRRPv2 版本只支持 IPv4 VRRP，VRRPv3 版本支持 IPv4 VRRP 和 IPv6 VRRP。

3.3.1 VRRP 的工作原理

一台 VRRP 路由器有唯一的标识为 VRID，其范围为 0～255。该路由器对外表现为唯一的虚拟 MAC 地址。路由器开启 VRRP 功能后，会根据优先级确定自己在备份组中的角色。优先级高的路由器称为主路由器，优先级低的路由器称为备份路由器。当两台优先级相同的路由器同时竞争 Master 时，比较接口 IP 地址的大小。接口地址大者当选为 Master，其他路由器作为备份路由器，随时监听 Master 的状态。

3.3.2 VRRP 的状态

VRRP 协议中定义了三种状态机：初始状态（Initialize）、活动状态（Master）、备份状态（Backup）。其中，只有处于活动状态的设备才可以转发那些发送到虚拟 IP 地址的报文。

3.3.3 VRRP 监视功能

1. 监视指定接口

VRRP 的监视指定接口功能更好地扩充了备份功能：不仅能在备份组中某路由器的接口出现故障时提供备份功能，还能在路由器的其他接口（如连接上行链路的接口）不可用时提供备份功能。

路由器连接上行链路的接口出现故障时，备份组无法感知上行链路接口的故障，如果该路由器此时处于 Master 状态，将会导致局域网内的主机无法访问外部网络。通过监视指定接口的功能，可以解决该问题。当连接上行链路的接口处于 Down 或 Removed 状态时，路由器主动降低自己的优先级，使得备份组内其他路由器的优先级高于这台路由器，以便优先级最高的路由器成为 Master，承担转发任务。

2. 监视 Track 项

通过 VRRP 监视 Track 项功能，可以根据上行链路的状态，改变路由器的优先级。当上行链路出现故障，局域网内的主机无法通过路由器访问外部网络时，被监视 Track 项的状态为 Negative，并将路由器的优先级降低指定的数额。从而使得备份组内其他路由器的优先级高于这台路由器的优先级，成为 Master 路由器，保证局域网内主机与外部网络的通信不会中断。

在 Backup 路由器上监视 Master 路由器的状态。当 Master 路由器出现故障时，工作在切换模式的 Backup 路由器能够迅速成为 Master 路由器，以保证通信不会中断。

3.3.4 VRRP 的配置命令

表 3-3 所示是配置 VRRP 时所需用到的一些命令。

表 3-3 VRRP 的配置命令

操作命令	操作说明
system-view	进入系统界面
int VLAN number	进入 VLAN 配置界面
IP address ×.×.×.× ×.×.×.×	配置 VLAN 的实际 IP 地址
VRRP vrid id virtual-ip ×.×.×.×	配置备份组 ID 的虚拟 IP 地址
VRRP vrid id priority number	配置备份组 ID 的优先级

实验 3 配置 VRRP

实验目的：学会解决网关冗余的问题。

实验器材：H3C S5820 两台。

实验要求：

S1 作为 VLAN 21 内主机的实际网关，S2 作为 VLAN 31 内主机的实际网关。其中，各 VRRP 组中高优先级设置为 150，低优先级设置为 120。

提示：为让同学们更加清晰地了解 VRRP 的配置，以下实验特地加了 VLAN 11 与 VLAN 31，但不将端口加入这两个 VLAN 网中。

实验拓扑：VRRP 的配置拓扑图如图 3-3 所示。



图 3-3　VRRP 的配置拓扑图

实验步骤如下：

```
[S1]vlan 11
[S1-vlan11]vlan 21
[S1-vlan21]vlan 31
[S1-vlan31]vlan 41
[S1]vlan 21
[S1-vlan21]port GigabitEthernet 1/0/1
[S1-vlan21]vlan 31
[S1-vlan31]port GigabitEthernet 1/0/2
[S1]int vlan 11
[S1-Vlan-interface11]ip add 10.10.10.253 24        //配置 VLAN 11 的实际 IP 地址
[S1-Vlan-interface11]vrrp vrid 10 virtual-ip 10.10.10.254
  //设置 VRRP 备份组号为 10,且 VRRP 虚拟 IP 为 10.10.10.254
[S1-Vlan-interface11]vrrp vrid 10 priority 150
  //设置 VRRP 备份组号 10 的优先级为 150
[S1-Vlan-interface11]int vlan 21
[S1-Vlan-interface21]ip address 10.10.20.253 24
  //配置 VLAN 21 的实际 IP 地址
[S1-Vlan-interface21]vrrp vrid 20 virtual-ip 10.10.20.254
  //设置 VRRP 备份组号为 20,且 VRRP 虚拟 IP 为 10.10.20.254
[S1-Vlan-interface21]vrrp vrid 20 priority 150
  //设置 VRRP 备份组号 20 的优先级为 150
[S1]int vlan 31
[S1-Vlan-interface31]ip address 10.10.30.253 24
[S1-Vlan-interface31]vrrp vrid 30 virtual-ip 10.10.30.254
[S1-Vlan-interface31]vrrp vrid 30 priority 120
  //设置 VRRP 备份组号 30 的优先级为 120
[S1-Vlan-interface31]int vlan 41
[S1-Vlan-interface41]ip address 10.10.40.253 24
[S1-Vlan-interface41]vrrp vrid 40 virtual-ip 10.10.40.254
[S1-Vlan-interface41]vrrp vrid 40 priority 120
  //设置 VRRP 备份组号 40 的优先级为 120

[S2]vlan 11
[S2-vlan11]vlan 21
```

```
[S2-vlan21]vlan 31
[S2-vlan31]vlan 41
[S2]vlan 21
[S2-vlan21]port GigabitEthernet 1/0/1
[S2-vlan21]vlan 31
[S2-vlan31]port GigabitEthernet 1/0/2
[S2]int vlan 11
[S2-Vlan-interface11]ip add 10.10.10.252 24
[S2-Vlan-interface11]vrrp vrid 10 virtual-ip 10.10.10.254
[S2-Vlan-interface11]vrrp vrid 10 priority 120
  //设置 VRRP 备份组号 10 的优先级为 120
[S2-Vlan-interface11]int vlan 21
[S2-Vlan-interface21]ip address 10.10.20.252 24
[S2-Vlan-interface21]vrrp vrid 20 virtual-ip 10.10.20.254
[S2-Vlan-interface21]vrrp vrid 20 priority 120
  //设置 VRRP 备份组号 20 的优先级为 120
[S2]int vlan 31
[S2-Vlan-interface31]ip address 10.10.30.252 24
[S2-Vlan-interface31]vrrp vrid 30 virtual-ip 10.10.30.254
[S2-Vlan-interface31]vrrp vrid 30 priority 150
  //设置 VRRP 备份组号 30 的优先级为 150
[S2-Vlan-interface31]int vlan 41
[S2-Vlan-interface41]ip address 10.10.40.252 24
[S2-Vlan-interface41]vrrp vrid 40 virtual-ip 10.10.40.254
[S2-Vlan-interface41]vrrp vrid 40 priority 150
  //设置 VRRP 备份组号 40 的优先级为 150
```

实验结果如下：

（1）

```
[S1]display vrrp verbose
IPv4 Virtual Router Information:
  Running mode : Standard
    Total number of virtual routers : 4
    Interface Vlan-interface11
      VRID             : 10          Adver Timer   : 100
      Admin Status     : Up          State         : Initialize
      Config Pri       : 150         Running Pri   : 150
      Preempt Mode     : Yes         Delay Time    : 0
      Auth Type        : None
      Virtual IP       : 10.10.10.254
      Master IP        : 0.0.0.0

      Interface Vlan-interface21
      VRID             : 20Adver Timer  : 100
      Admin Status     : Up          State         : Master
      Config Pri       : 150         Running Pri   : 150
      Preempt Mode     : Yes         Delay Time    : 0
      Auth Type        : None
      Virtual IP       : 10.10.20.254
```

```
    Virtual MAC       : 0000-5e00-0114
    Master IP         : 10.10.20.253

    Interface Vlan-interface31
    VRID              : 30              Adver Timer  : 100
    Admin Status      : Up              State        : Backup
    Config Pri        : 120             Running Pri  : 120
    Preempt Mode      : Yes             Delay Time   : 0
    Become Master     : 3400ms left
    Auth Type         : None
    Virtual IP        : 10.10.30.254
    Master IP         : 10.10.30.252

    Interface Vlan-interface41
    VRID              : 40              Adver Timer  : 100
    Admin Status      : Up              State        : Initialize
    Config Pri        : 120             Running Pri  : 120
    Preempt Mode      : Yes             Delay Time   : 0
    Auth Type         : None
    Virtual IP        : 10.10.40.254
    Master IP         : 0.0.0.0
```

（2）

```
[S2]display vrrp verbose
IPv4 Virtual Router Information:
  Running mode: Standard
   Total number of virtual routers: 4
   Interface Vlan-interface11
    VRID              : 10              Adver Timer  : 100
    Admin Status      : Up              State        : Initialize
    Config Pri        : 120             Running Pri  : 120
    Preempt Mode      : Yes             Delay Time   : 0
    Auth Type         : None
    Virtual IP        : 10.10.10.254
    Master IP         : 0.0.0.0

    Interface Vlan-interface21
    VRID              : 20              Adver Timer  : 100
    Admin Status      : Up              State        : Backup
    Config Pri        : 120             Running Pri  : 120
    Preempt Mode      : Yes             Delay Time   : 0
    Become Master     : 3340ms left
    Auth Type         : None
    Virtual IP        : 10.10.20.254
    Master IP         : 10.10.20.253

    Interface Vlan-interface31
    VRID              : 30              Adver Timer  : 100
    Admin Status      : Up              State        : Master
```

```
Config Pri          : 150           Running Pri   : 150
Preempt Mode        : Yes           Delay Time    : 0
Auth Type           : None
Virtual IP          : 10.10.30.254
Virtual MAC         : 0000-5e00-011e
Master IP           : 10.10.30.252

Interface Vlan-interface41
VRID                : 40            Adver Timer   : 100
Admin Status        : Up            State         : Initialize
Config Pri          : 150           Running Pri   : 150
Preempt Mode        : Yes           Delay Time    : 0
Auth Type           : None
Virtual IP          : 10.10.40.254
Master IP           : 0.0.0.0
```

3.4 IRF 简介

IRF 是 Intelligent Resilient Framework 的缩写，意思为智能弹性架构，它通过一些配置，将多台连接在一起的设备虚拟化成一台“设备”。使用这种技术，有利于用户的管理与维护。

3.4.1 IRF 的工作原理

IRF 要正常工作，需先在成员设备间通过 IRF 物理连接端口进行物理连接，再在设备上设置成员编号并进行成员选举。通常情况下，优先级最大的作为 Master(主设备)，其他的作为 Slave(从设备)。若未设定优先级，则自动选举 Master 及 Slave。

3.4.2 IRF 的访问

1. 访问 Master

IRF 的访问方式如下。

本地登录：通过任意成员设备的 AUX 或者 Console 口登录。

远程登录：给任意成员设备的任意三层接口配置 IP 地址，并且路由可达，就可以通过 Telnet、Web、SNMP 等方式进行远程登录。

2. 访问 Slave

用户访问 IRF 时，实际访问的是 IRF 中的 Master 设备，访问终端的操作界面显示的是 Master 设备的控制台。需要重定向到 Slave 设备，才能登录到 Slave 设备。

不管使用哪种方式登录 IRF，实际上登录的都是 Master。Master 是 IRF 系统的配置

和控制中心，在 Master 上配置后，Master 会将相关配置同步给 Slave，以便保证 Master 和 Slave 配置的一致性。

3.4.3 MAD 的配置

MAD 检测分为 BFD MAD 检测和 LACP MAD 检测。其中，BFD MAD 检测方式可以在直连设备间实现，也可以使用中间设备来进行检测，而 LACP MAD 检测方式必须使用中间设备。

LACP MAD 检测配置如下：

```
interface bridge-aggregation              //进入二层聚合端口视图
link-aggregation mode dynamic             //配置聚合组工作模式为动态聚合模式
mad enable                                //开启 LACP MAD 检测
功能 Interface                            //进入端口
port link-aggregation group               //将以太网端口加入聚合
```

BFD MAD 检测配置如下：

```
vlan                                      //创建一个新 VLAN 并专用于 BFD
MAD 检测 Interface                        //进入端口
Port number                               //在 VLAN 下加入端口
interface vlan-interface                  //进入 VLAN 网
mad bfd enable                            //开启 BFD MAD 检测
mad ip address                            //给指定成员设备配置 MAD IP 地址
```

3.4.4 IRF 的配置命令

表 3-4 所示是配置 IRF 时所需用到的一些命令。

表 3-4 IRF 的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
interface Ten-GigabitEthernet number	进入 IRF 物理端口
shutdown	关闭端口
irf member number renumber number	设置成员编号
irf-port number/number	创建 IRF 端口
port group interface Ten-GigabitEthernet number	将 IRF 物理端口加入 IRF 端口
irf domain number	配置 IRF 域的编号
irf member numberpriority number	为成员设置优先级
irf-port-configuration active	激活 IRF 域

实验 4 配 置 IRF

实验目的：学会 IRF 的配置，知道如何简便地管理网络。

实验器材：H3C S5820 两台、Ten-GigabitEthernet 一条。

实验要求：

(1) 链形堆叠，IRF Domain 值为 10。

(2) S1 为 IRF 中的主设备，优先级值为 10。

(3) MAD 所使用的端口为交换机的第 23 个端口，检测 IP 为 100.0.0.1/30(member 1)和 100.0.0.2/30(member 2)，检测 VLAN 为 1000；Sysname 名称为 HQ-IRF。

IRF 的配置拓扑图如图 3-4 所示。



图 3-4 IRF 的配置拓扑图

实验步骤如下：

(1) 先在 S5820V2_1 上配置。

```
[H3C]hostname HQ-IRF
[HQ-IRF]interface Ten-GigabitEthernet 1/0/49
[HQ-IRF-Ten-GigabitEthernet1/0/49]shut                //将端口关闭
[HQ-IRF-Ten-GigabitEthernet1/0/49]quit
[HQ-IRF]irf-port 1/2                                  //创建 IRF 端口
[HQ-IRF-irf-port1/2]port group interface Ten-GigabitEthernet 1/0/49
  //将物理端口 Ten-GigabitEthernet1/0/49 加入 IRF 端口中
[HQ-IRF-irf-port1/2]quit
[HQ-IRF]interface Ten-GigabitEthernet 1/0/49
[HQ-IRF-Ten-GigabitEthernet1/0/49]undo shutdown       //开启端口
[HQ-IRF-Ten-GigabitEthernet1/0/49]quit
[HQ-IRF]irf domain 10                                 //配置 IRF 域的编号
[HQ-IRF]irf member 1 priority 10                      //配置优先级
[HQ-IRF]irf-port-configuration active                 //激活 IRF 在 S5820
```

(2) 在 S5820V2_2 上配置。

```
[H3C]hostname HQ-IRF
[HQ-IRF]irf member 1 renumber 2                       //将设备的成员编号修改为 2
[HQ-IRF]quit
<HQ-IRF> reboot                                       //重启，让成员编号生效
[HQ-IRF]interface Ten-GigabitEthernet 2/0/49
```

```
[HQ-IRF-Ten-GigabitEthernet2/0/49]shutdown
[HQ-IRF]irf-port 2/1                                    //创建 IRF 端口
[HQ-IRF-irf-port2/1]port group interface Ten-GigabitEthernet 2/0/49
[HQ-IRF-irf-port2/1]quit
[HQ-IRF]interface Ten-GigabitEthernet 2/0/49
[HQ-IRF-Ten-GigabitEthernet2/0/49]undo shutdown
[HQ-IRF]save                                             //保存数据,以免重启系统时数据丢失
[HQ-IRF]irf-port-configuration active              //激活 IRF
```

（3）配置 BFD MAD 检测。

```
[HQ-IRF]vlan 1000
[HQ-IRF-vlan1000]quit
[HQ-IRF]interface Vlan-interface 1000
[HQ-IRF-Vlan-interface1000]mad bfd enable               //开启 BFD MAD 检测
[HQ-IRF-Vlan-interface1000]mad ip address 100.0.0.1 30 member 1   //设置检测 IP
[HQ-IRF-Vlan-interface1000]mad ip address 100.0.0.2 30 member 2
[HQ-IRF]vlan 1000
[HQ-IRF-vlan1000]port GigabitEthernet 1/0/23            //加入端口
```

实验结果如下：

```
[HQ-IRF]display irf
MemberID  Role     Priority    CPU-Mac       Description
   *1     Master      10      ac51-c2d9-0104    ---
   +2     Standby     1       ac41-4bbf-0204    ---
-------------------------------------------------------------
* indicates the device is the master.
+ indicates the device through which the user logs in.


The bridge MAC of the IRF is : ac51-c2d9-0100
Auto upgrade                 : yes
Mac persistent               : 6 min
Domain ID                    : 10
[HQ-IRF]display mad verbose Multi-active
recovery state : No Excluded ports (user-configured)
               : Excluded ports (system-configured)
               : Ten-GigabitEthernet1/0/49
Ten-GigabitEthernet2/0/49
MAD ARP disabled. MAD ND disabled. MAD LACP disabled.
MAD BFD enabled interface : Vlan-interface1000
MAD status                : Faulty
Member ID  MAD IP address  Neighbor  MAD status
    1       100.0.0.1/30      2        Faulty
    2       100.0.0.2/30      1        Faulty
```

3.5 GVRP 简 介

GARP(Generic Attribute Registration Protocol,通用属性注册协议)作为一个属性注册协议的载体,可以用来传播属性。遵循 GARP 的应用实体称为 GARP 应用。

GVRP(GARP VLAN Registration Protocol,GARP VLAN 注册协议)就是 GARP 的应用之一,用于注册和注销 VLAN 属性。

3.5.1 GVRP 的注册模式

GVRP 有三种注册模式,不同注册模式对静态 VLAN 和动态 VLAN 的处理方式也不同。我们将通过手动创建的 VLAN,称为静态 VLAN,通过 GVRP 创建的 VLAN,称为动态 VLAN。

(1) Normal 模式。该模式下的端口允许进行动态 VLAN 的注册或注销,并允许发送动态和静态 VLAN 的声明。

(2) Fixed 模式。该模式下的端口禁止进行动态 VLAN 的注册或注销,且只允许发送静态 VLAN 的声明。也就是说,该模式下的 Trunk 端口即使允许所有 VLAN 通过,实际通过的 VLAN 也只能是手动创建的那部分 VLAN。

(3) Forbidden 模式。该模式下的端口禁止进行动态 VLAN 的注册或注销,且只允许发送 VLAN 1 的声明。也就是说,该模式下的 Trunk 端口即使允许所有 VLAN 通过,实际通过的 VLAN 也只能是 VLAN 1。

3.5.2 GVRP 的配置命令

表 3-5 所示是配置 GVRP 时所需用到的一些命令。

表 3-5 GVRP 的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
int number	进入端口
gvrp	为端口开启 GVRP
gvrp registration fixed	设置端口模式为 Fixed
gvrp registration forbidden	设置端口模式为 Forbidden

实验 5 配置 GVRP Normal 注册模式

实验目的:掌握 Normal 的注册模式,知道如何实现交换机之间 VLAN 的注册和注销。

实验器材：H3C S5800 两台。

实验要求：配置 GVRP 的注册模式为 Normal，实现 S1 和 S2 之间所有动态与静态 VLAN 的注册和注销。

GVRP Normal 的配置拓扑图如图 3-5 所示。



图 3-5　GVRP Normal 的配置拓扑图

实验步骤如下：

```
[S1]GVRP                                   //全局模式下开启 GVRP 功能
[S1]interface GigabitEthernet 1/0/1
[S1-GigabitEthernet1/0/1]port link-type trunk
[S1-GigabitEthernet1/0/1]port trunk permit vlan all
[S1-GigabitEthernet1/0/1]gvrp              //为端口开启 GVRP
[S1-GigabitEthernet1/0/1]quit
[S1]vlan 10
[S1-vlan10]quit
[S2]gvrp
[S2]interface GigabitEthernet 1/0/1
[S2GigabitEthernet1/0/1port link-type trunk
[S2GigabitEthernet1/0/1]port trunk permit vlan all
[S2GigabitEthernet1/0/1]gvrp
[S2-GigabitEthernet1/0/1]quit
[S2]vlan 20
[S2-vlan20]quit
```

实验结果如下：

```
[S1]display gvrp local-vlan
interface GigabitEthernet 1/0/1
Following VLANs exist in GVRP local database:
1(default), 10, 20,

[S2]display gvrp local-vlan interface GigabitEthernet 1/0/1
Following VLANs exist in GVRP local database:
1(default), 10, 20,
```

实验 6　配置 GVRP Fixed 注册模式

实验目的：掌握 Fixed 的注册模式，知道如何实现交换机之间 VLAN 的注册和注销。

实验器材：H3C S5800 两台。

实验要求：配置 GVRP 的注册模式为 Fixed，实现 S1 和 S2 之间所有静态 VLAN 的

注册和注销。

GVRP Fixed 的配置拓扑图如图 3-6 所示。



图 3-6　GVRP Fixed 的配置拓扑图

实验步骤如下：

```
[S1]GVRP                                                    //全局模式下开启 GVRP 功能
[S1]interface GigabitEthernet 1/0/1
[S1-GigabitEthernet1/0/1]port link-type trunk
[S1-GigabitEthernet1/0/1]port trunk permit vlan all
[S1-GigabitEthernet1/0/1]gvrp                               //为端口开启 GVRP
[S1-GigabitEthernet1/0/1]gvrp registration fixed            //设置端口模式为 Fixed
[S1-GigabitEthernet1/0/1]quit
[S1]vlan 10
[S1-vlan10]quit
[S2]gvrp
[S2]interface GigabitEthernet 1/0/1
[S2-GigabitEthernet1/0/1]port link-type trunk
[S2-GigabitEthernet1/0/1]port trunk permit vlan all
[S2-GigabitEthernet1/0/1]gvrp
[S2-GigabitEthernet1/0/1]gvrp registration fixed
[S2-GigabitEthernet1/0/1]quit
[S2]vlan 20
[S2-vlan20]quit
```

实验结果如下：

```
[S1]display gvrp local-vlan interface GigabitEthernet 1/0/1
    Following VLANs exist in GVRP local database:
1(default), 10,

[S2]display gvrp local-vlan interface GigabitEthernet 1/0/1
    Following VLANs exist in GVRP local database:
1(default), 20,
```

实验 7　配置 GVRP Forbidden 注册模式

实验目的：掌握 GVRP Forbidden 的配置方法。

实验器材：H3C S5800 两台。

实验要求：配置 GVRP 的注册模式为 Forbidden，来阻止 S1 和 S2 之间除 VLAN 1 以外所有 VLAN 的注册和注销。

GVRP Forbidden 的配置拓扑图如图 3-7 所示。



图 3-7 GVRP Forbidden 的配置拓扑图

实验步骤如下：

```
[S1]GVRP                                 //全局模式下开启 GVRP 功能
[S1]interface GigabitEthernet 1/0/1
[S1-GigabitEthernet1/0/1]port link-type trunk
[S1-GigabitEthernet1/0/1]port trunk permit vlan all
[S1-GigabitEthernet1/0/1]gvrp            //为端口开启 GVRP
[S1-GigabitEthernet1/0/1]gvrp registration forbidden
  //设置端口模式为 Forbidden
[S1-GigabitEthernet1/0/1]quit
[S1]vlan 10
[S1-vlan10]quit
[S2]gvrp
[S2]interface GigabitEthernet 1/0/1
[S2-GigabitEthernet1/0/1]port link-type trunk
[S2-GigabitEthernet1/0/1]port trunk permit vlan all
[S2-GigabitEthernet1/0/1]gvrp
[S2-GigabitEthernet1/0/1]gvrp registration forbidden
[S2-GigabitEthernet1/0/1]quit
[S2]vlan 20
[S2-vlan20]quit
```

实验结果如下：

```
[S1]display gvrp local-vlan interface GigabitEthernet 1/0/1
    Following VLANs exist in GVRP local database:
1(default)

[S2]display gvrp local-vlan interface GigabitEthernet 1/0/1
    Following VLANs exist in GVRP local database:
1(default)
```

项目4　广域网接入

4.1　PPP简介

PPP(Point to Point Protocol,点对点协议)是一种用来同步调制连接的数据链路层协议。它能够提供用户认证和支持同步串行介质和异步串行介质,并且PPP还使用了链路控制协议(Link Control Protocol,LCP)和网络控制协议(Network Control Protocol,NCP)。

4.1.1　PPP认证方式

为保证链路上的安全,PPP提供了在其链路上进行安全认证的手段,使得在PPP链路上实施AAA(*Authentication*、*Authorization*、*Accounting*,认证、授权和记账)协议变得切实可行。PPP有两种认证方式,一种是PAP(Password Authentication Protocol,密码认证协议)认证;另一种是CHAP(Challenge Handshake Authentication Protocol,询问握手认证协议)认证。PAP为两次握手协议,它通过用户名和密码来对用户进行认证。CHAP为三次握手协议,它分为认证方配置了用户名和认证方没有配置用户名两种情况。PAP在传输用户名和密码时用明文,而CHAP在传输过程中不传输密码,只传输用户名,所以,CHAP的安全性会比PAP的安全性高。

4.1.2　PPP的配置命令

表4-1所示是配置PPP时所需用到的一些命令。

表4-1　PPP的配置命令

操作命令	操作说明
system-view	进入系统界面
int serial number	进入串行口
ppp authentication-mode chap	设置验证方式为CHAP
ppp chap user name	设置用户名
ppp chap password simple number	设置明文密码
ppp chap password cipher number	设置密文密码

实验 1 配 置 PPP

实验目的：学会 PPP 的配置，掌握 CHAP 的认证方式。

实验器材：H3C MSR36-20 两台。

实验要求：

- 使用 CHAP 认证。
- 用户名和密码均为 123456。

PPP 的配置及 CHAP 的认证拓扑图如图 4-1 所示。



图 4-1 PPP 的配置及 CHAP 的认证拓扑图

实验步骤如下：

```
[R1]interface Serial 1/0
[R1-Serial1/0]ip address 192.168.1.1 24
[R1]local-user 123456 class network              //创建本地账号 123456
[R1-luser-network-123456]password simple 123456   //设置本地密码为 123456
[R1-luser-network-123456]service-type ppp         //设置本地用户的服务类型为 PPP
[R1-luser-network-123456]quit
[R1]domain system
[R1-isp-system]authentication ppp local
[R1-isp-system]quit
[R1]interface Serial 1/0
[R1-Serial1/0]ppp authentication-mode chap domain system
  //设置 R1 的本地认证方式为 CHAP
[R1-Serial1/0]ppp chap user 123456
  //设置采用 CHAP 时 R1 的用户名为 123456
[R1-Serial1/0]ppp chap password simple 123456

[R2]interface Serial 1/0
[R2-Serial1/0]ip add 192.168.1.2 24
[R2]local-user 123456 class network
[R2-luser-network-123456]password simple 123456
[R2-luser-network-123456]quit
[R2]domain system
[R2-isp-system]authentication ppp local
[R2-isp-system]quit
[R2]interface Serial 1/0
[R2-Serial1/0]ppp authentication-mode chap domain system
[R2-Serial1/0]ppp chap user 123456
[R2-Serial1/0]ppp chap password simple 123456
```

实验结果如下：

```
[R1]display interface Serial 1/0
Serial1/0
Current state: UP
Line protocol state:
UP Description: Serial1/0 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 192.168.1.1/24 (primary)
Link layer protocol: PPP
LCP: opened, IPCP: stopped
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: 0 hours 9 minutes 4 seconds
Last clearing of counters: Never

[R2]display interface Serial 1/0
Serial1/0
Current state: UP Line
protocol state: UP
Description: Serial1/0 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 192.168.1.2/24 (primary)
Link layer protocol: PPP
LCP: opened, IPCP: opened
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: 0 hours 28 minutes 24 seconds
Last clearing of counters: Never

[R1]ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=0.000 ms

---Ping statistics for 192.168.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss round-
trip min/avg/max/std-dev =0.000/0.200/1.000/0.400 ms
[R1]% Feb 2 21:42:55:617 2017 R1 PING/6/PING_STATISTICS: Ping statistics for
192.168.1.2: 5 packet(s) tra ted, 5 packet(s) received, 0.0% packet loss, round-trip min/
```

```
avg/max/std-dev = 0.000/0.200/1.000/0.400 ms

[R2]ping 192.168.1.1
Ping 192.168.1.1 (192.168.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.000 ms

---Ping statistics for 192.168.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss round-trip min/avg/max/std
-dev = 0.000/0.200/1.000/0.400 ms
[R2]% Feb 2 21:43:59:186 2017 R2 PING/6/PING_STATISTICS: Ping statistics for
192.168.1.1: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip
min/avg/max/std-dev = 0.000/0.200/1.000/0.400 ms
```

4.2　HDLC 简 介

HDLC(High-level Data Link Control,高级数据链路控制)是一种面向比特的数据链路层协议,它具有透明性、帧格式、规程种类的特点。

4.2.1　HDLC 的基本概念

HDLC 捆绑:HDLC 捆绑是一组 HDLC 接口的集合,HDLC 捆绑是随着 HDLC 捆绑接口的创建而自动生成的,其编号与 HDLC 捆绑接口编号相同。

HDLC 捆绑接口:HDLC 捆绑接口是一个逻辑接口,一个 HDLC 捆绑接口对应一个 HDLC 捆绑。

成员接口:加入 HDLC 捆绑后的接口称为成员接口。

目前,只有 POS 接口和 Serial 接口可以加入 HDLC 捆绑,并且加入 HDLC 捆绑的成员接口的数据链路层协议类型必须是 HDLC。

加入 HDLC 捆绑后,成员接口的网络层将被置于 Down 状态,成员接口上的三层业务相关的配置都不生效,成员接口通过 HDLC 捆绑接口的三层配置进行业务处理。

4.2.2　HDLC 与 PPP 的区别

(1) HDLC 协议只支持点到点链路,不支持点到多点链路。

(2) HDLC 只能封装在同步链路上,如果是同异步串口,只有当同异步串口工作在同步模式下才能使用;而 PPP 可以使用在异步串行连接,如拨号或者同步串行连接,如 ISDN。

(3) PPP 是面向字符的,HDLC 是面向位的。

4.2.3 HDLC 的配置命令

表 4-2 所示是配置 HDLC 时所需用到的一些命令。

表 4-2 HDLC 的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
interface hdlc-bundle number	创建 HDLC 捆绑组
ip address ×.×.×.× ×.×.×.×	设置捆绑组的 IP 地址
int number	进入端口配置界面
link-protocol hdlc	封装 HDLC
bundle id number	将端口加入 HDLC 捆绑组中

实验 2 配 置 HDLC

实验目的:

(1) 掌握 HDLC 的配置方法。

(2) 了解 HDLC 的原理。

实验器材:H3C MSR36-20 两台。

实验要求:为了增加 R1 和 R2 之间的链路带宽,并提高连接可靠性,在设备之间建立 HDLC 捆绑逻辑链路。

HDLC 的配置拓扑图如图 4-2 所示。



图 4-2 HDLC 的配置拓扑图

实验步骤如下:

```
[R1] interface hdlc-bundle 1                    //创建 HDLC 捆绑 1
[R1-HDLC-bundle1] ip address 10.10.10.1 24
[R1]interface Serial 1/0
[R1-Serial1/0]link-protocol hdlc                //封装 HDLC 协议
[R1-Serial1/0]bundle id 1                       //将端口加入 HDLC 捆绑 1
[R1]interface Serial 2/0
[R1-Serial2/0]link-protocol hdlc
[R1-Serial2/0]bundle id 1
```

```
[R1] interface hdlc-bundle 1
[R1-HDLC-bundle1] ip address 10.10.10.2 24
[R2]interface Serial 1/0
[R2-Serial1/0]link-protocol hdlc
[R2-Serial1/0]bundle id 1
[R2]interface Serial 2/0
[R2-Serial2/0]link-protocol hdlc
[R2-Serial2/0]bundle id 1
```

实验结果如下：

```
[R1]display bundle hdlc-bundle
Bundle: HDLC-bundle1,
  Selected members: 0, Total bandwidth: 0 kbps
    Member        State     Bandwidth(kbps)    Priority
  Serial1/0     Initial          64             32768
  Serial2/0     Initial          64             32768

[R2]display bundle hdlc-bundle
Bundle: HDLC-bundle1,
  Selected members: 0, Total bandwidth: 0 kbps
    Member        State     Bandwidth(kbps)    Priority
  Serial1/0     Initial          64             32768
  Serial2/0     Initial          64             32768

[R1]ping 10.10.10.2
Ping 10.10.10.2 (10.10.10.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.10.10.2: icmp_seq=0 ttl=255 time=0.000 ms
56 bytes from 10.10.10.2: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.10.10.2: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 10.10.10.2: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 10.10.10.2: icmp_seq=4 ttl=255 time=2.000 ms

---Ping statistics for 10.10.10.2---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss round-
trip min/avg/max/std-dev =0.000/0.800/2.000/0.748 ms
[H3C]%Feb 2 22:38:15:142 2017 H3C PING/6/PING_STATISTICS: Ping statistics for
10.10.10.2: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip
min/avg/max/std-dev =0.000/0.800/2.000/0.748 ms

[R2]ping 10.10.10.1
Ping 10.10.10.1 (10.10.10.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.10.10.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 10.10.10.1: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 10.10.10.1: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 10.10.10.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 10.10.10.1: icmp_seq=4 ttl=255 time=1.000 ms
```

```
---Ping statistics for 10.10.10.1---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss round-
trip min/avg/max/std-dev =0.000/1.000/2.000/0.632 ms
[R2]% Feb 2 22:38:37:255 2017 R2 PING/6/PING_STATISTICS: Ping statistics for
10.10.10.1: 5 packet(s) transmitted, 5 packet(s) received, 0.0%  packet loss,round-trip
min/avg/max/std-dev =0.000/1.000/2.000/0.632 ms
```

项目 5　路由规划及应用

5.1　静 态 路 由

静态路由是指需要由用户或管理员手动配置路由信息的一种特殊路由。静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

5.1.1　静态路由的特点

静态路由主要有手动配置、路由路径相对固定、永久存在、不可通告性、单向性、接力性、递归性、优先级较高、使用小型网络等特点。

5.1.2　默认路由

默认路由是一种特殊的静态路由。如果没有默认路由，那么目的地址在路由表中没有匹配表项的包将被丢弃，通过给当前路由器配置一条默认路由，那些在路由表里找不到匹配路由表入口项的数据报文将会转发给另外一台路由器(如果这台路由器的路由能力比较强，包括到达大部分所有网络的路由信息)，由另外一台路由器进行报文的转发。

5.1.3　静态路由的配置命令

表 5-1 所示是配置静态路由时所需用到的一些命令。

表 5-1　静态路由的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
int number	进入端口配置界面
ip address ×.×.×.× ×.×.×.×	设置 IP 地址
ip route-static ×.×.×.× ×.×.×.× ×.×.×.×	设置静态路由
ip route-static 0.0.0.0 0.0.0.0 ×.×.×.×	设置默认路由

实验 1　配置静态路由

实验目的：掌握静态路由的配置方法，学会应用于简单的网络环境中。

实验器材：H3C MSR36-20 两台、PC 两台。

静态路由的配置拓扑图如图 5-1 所示。

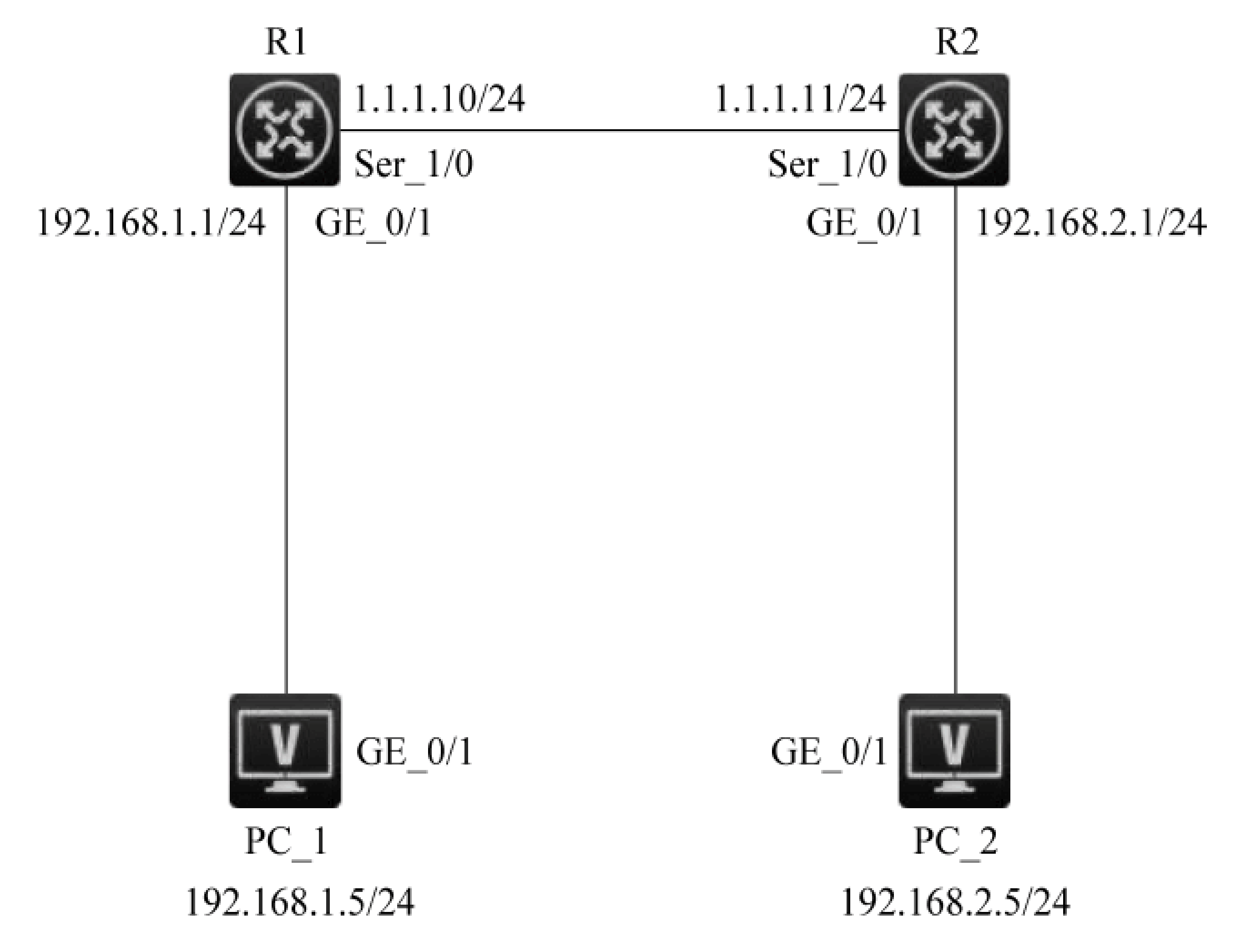


图 5-1　静态路由的配置拓扑图

实验步骤如下：

```
[R1]interface Serial 1/0
[R1-Serial1/0]ip address 1.1.1.10 24
[R1]interface GigabitEthernet 0/1
[R1-GigabitEthernet0/1]ip address 192.168.1.1 24
[R1-GigabitEthernet0/1]quit
[R1]ip route-static 192.168.2.1 255.255.255.0 1.1.1.11      //配置静态路由
[R2]interface Serial 1/0
[R2-Serial1/0]ip address 1.1.1.11 24
[R2]interface GigabitEthernet 0/1
[R2-GigabitEthernet0/1]ip address 192.168.2.1 24
[R2-GigabitEthernet0/1]quit
[R2]ip route-static 192.168.1.1 255.255.255.0 1.1.1.10      //配置静态路由
```

1）在 PC_1 上配置

在 PC_1 上配置静态路由的效果如图 5-2 所示。

2）在 PC_2 上配置

在 PC_2 上配置静态路由的效果如图 5-3 所示。



图 5-2　在 PC_1 上配置静态路由的效果



图 5-3　在 PC_2 上配置静态路由的效果

实验结果如下：

（1）在 PC_1 上 ping PC_2 的 IP 地址。

```
[H3C]ping 192.168.2.5
Ping 192.168.2.5 (192.168.2.5): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.2.5: icmp_seq=0 ttl=253 time=2.000 ms
56 bytes from 192.168.2.5: icmp_seq=1 ttl=253 time=2.000 ms
56 bytes from 192.168.2.5: icmp_seq=2 ttl=253 time=2.000 ms
56 bytes from 192.168.2.5: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 192.168.2.5: icmp_seq=4 ttl=253 time=1.000 ms

---Ping statistics for 192.168.2.5---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss round-
trip min/avg/max/std-dev =1.000/1.800/2.000/0.400 ms
[H3C]%Feb 14 15:58:23:973 2017 H3C PING/6/PING_STATISTICS: Ping statistics for
192.168.2.5: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip
min/avg/max/std-dev =1.000/1.800/2.000/0.400 ms
```

（2）在 PC_2 上 ping PC_1 的 IP 地址。

```
[H3C]ping 192.168.1.5
Ping 192.168.1.5 (192.168.1.5): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.5: icmp_seq=0 ttl=253 time=4.000 ms
56 bytes from 192.168.1.5: icmp_seq=1 ttl=253 time=2.000 ms
56 bytes from 192.168.1.5: icmp_seq=2 ttl=253 time=2.000 ms
56 bytes from 192.168.1.5: icmp_seq=3 ttl=253 time=1.000 ms
56 bytes from 192.168.1.5: icmp_seq=4 ttl=253 time=1.000 ms

---Ping statistics for 192.168.1.5---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss round-trip min/avg/max/std
-dev =1.000/2.000/4.000/1.095 ms
[H3C]%Feb 14 16:00:36:864 2017 H3C PING/6/PING_STATISTICS: Ping statistics for
192.168.1.5: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip
min/avg/max/std-dev =1.000/2.000/4.000/1.095 ms
```

5.2 IS-IS 简介

IS-IS(Intermediate System to Intermediate System Routing Protocol,中间系统到中间系统的路由选择协议)是一种链路状态协议。IS-IS 使用 LSP(Link State PDU)维护一个链路状态数据库。

5.2.1 IS-IS 区域

（1）Level-1 路由器。Level-1 路由器负责区域内的路由,它只与属于同一区域的 Level-1 和 Level-1-2 路由器形成邻居关系,维护一个 Level-1 的 LSDB,该 LSDB 包含本

区域的路由信息，到区域外的报文转发给最近的 Level-1-2 路由器。属于不同区域的 Level-1 路由器不能形成邻居关系。

(2) Level-2 路由器。Level-2 路由器负责区域间的路由，可以与同一区域或者其他区域的 Level-2 和 Level-1-2 路由器形成邻居关系，维护一个 Level-2 的 LSDB，该 LSDB 包含区域间的路由信息。所有 Level-2 路由器和 Level-1-2 路由器组成路由域的骨干网，负责在不同区域间通信，骨干网必须是物理连续的。Level-2 路由器是否形成邻居关系与区域无关。

(3) Level-1-2 路由器。同时属于 Level-1 和 Level-2 的路由器称为 Level-1-2 路由器，可以与同一区域的 Level-1 和 Level-1-2 路由器形成 Level-1 的邻居关系，也可以与同一区域或者其他区域的 Level-2 和 Level-1-2 路由器形成 Level-2 的邻居关系。Level-1 路由器必须通过 Level-1-2 路由器才能连接至其他区域。Level-1-2 路由器维护两个 LSDB，Level-1 的 LSDB 用于区域内路由，Level-2 的 LSDB 用于区域间路由。

5.2.2　IS-IS 的配置命令

表 5-2 所示是配置 IS-IS 时所需用到的一些命令。

表 5-2　IS-IS 的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
isis id	创建 IS-IS，并进入 IS-IS 配置界面
is-level level-number	设置路由等级
network-entity ××.0000.0000.000×.00	设置 IS-IS 的区域
int number	进入端口配置界面
isis enable id	启用 IS-IS

实验 2　配 置 IS-IS

实验目的：掌握 IS-IS 的配置方法。

实验器材：H3C MSR36-20 三台。

实验要求：IS-IS 进程为 10，R1 的区域为 10，R2、R3 的区域为 20，路由器等级为 Level-2。

IS-IS 的配置拓扑图如图 5-4 所示。

实验步骤如下：

```
[R1]isis 10                                   //创建 IS-IS 的进程号 10
[R1-isis-10]is-level level-2                  //设置路由等级为 Level-2
[R1-isis-10]network-entity 10.0000.0000.0001.00   //设置 IS-IS 的区域为 10
```

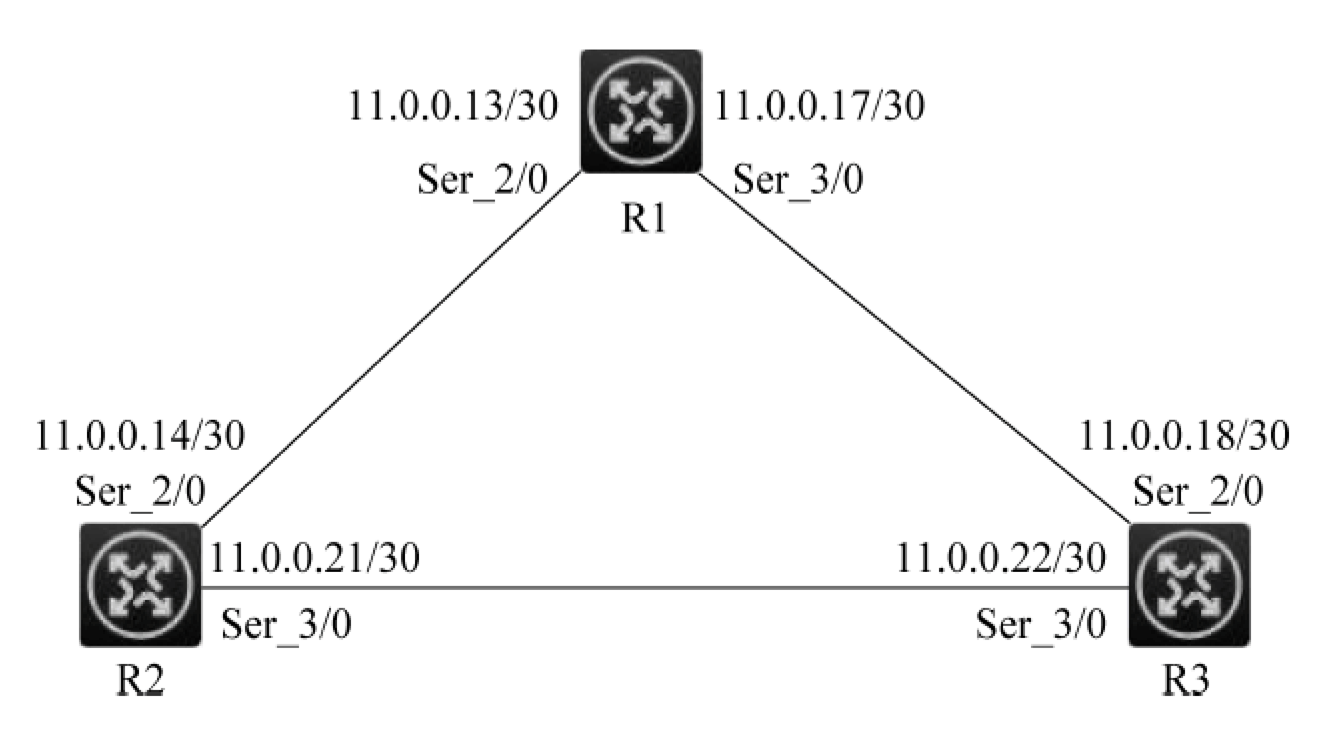


图 5-4　IS-IS 的配置拓扑图

```
[R1]interface Serial 2/0
[R1-Serial2/0]isis enable 10                          //在端口上启用 IS-IS
[R1-Serial2/0]quit
[R1]interface Serial3/0
[R1-Serial3/0]isis enable 10
[R2]isis 10
[R2-isis-10]is-level level-2
[R2-isis-10]network-entity 20.0000.0000.0002.00       //设置 IS-IS 的区域为 20
[R2-isis-10]quit
[R2]interface Serial 2/0
[R2-Serial2/0]isis enable 10
[R2-Serial2/0]quit
[R2]interface Serial3/0
R2-Serial3/0]isis enable 10
[R3]isis 10
[R3-isis-10]is-level level-2
[R3-isis-10]network-entity 20.0000.0000.0003.00
[R3-isis-10]quit
[R3]interface Serial 2/0
[R3-Serial2/0]isis enable 10
[R3-Serial2/0]quit
[R3]interface Serial 3/0
[R3-Serial3/0]isis enable 10
```

实验结果如下：

```
[R1]display isis lsdb

                         Database information for IS-IS(10)
                        ----------------------------------

                              Level-2 Link State Database
                           ----------------------------

LSPID                          Seq Num     Checksum  Holdtime   Length   ATT/P/OL
--------------------------------------------------------------------------------
```

```
0000.0000.0001.00-00*   0x00000007   0x6857     1135       95      0/0/0
0000.0000.0002.00-00    0x00000007   0xecb9     1143       95      0/0/0
0000.0000.0003.00-00    0x00000006   0xdbc2     1143       95      0/0/0
*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
[R2]display isis lsdb

                        Database information for IS-IS(10)
                       -----------------------------------

                            Level-2 Link State Database
                           ----------------------------

LSPID                      Seq Num     Checksum  Holdtime  Length  ATT/P/OL
---------------------------------------------------------------------------------
0000.0000.0001.00-00    0x00000007   0x6857     1052       95      0/0/0
0000.0000.0002.00-00*   0x00000007   0xecb9     1062       95      0/0/0
0000.0000.0003.00-00    0x00000006   0xdbc2     1061       95      0/0/0

*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
[R3]display isis lsdb

                        Database information for IS-IS(10)
                       -----------------------------------

                            Level-2 Link State Database
                           ----------------------------

LSPID                      Seq Num     Checksum  Holdtime  Length  ATT/P/OL
---------------------------------------------------------------------------------
0000.0000.0001.00-00    0x00000007   0x6857     1026       95      0/0/0
0000.0000.0002.00-00    0x00000007   0xecb9     1033       95      0/0/0
0000.0000.0003.00-00*   0x00000006   0xdbc2     1036       95      0/0/0

*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
```

5.3 BGP 简 介

BGP(Border Gateway Protocol,边界网关协议)是运行于 TCP 上的一种自治系统的路由协议,它可以应用于不同的 AS(Autonomous System,自治系统)之间,也可以应用于同一 AS 内部。当 BGP 运行于同一 AS 内部时,被称为 IBGP(Internal BGP);当 BGP 运行于不同 AS 之间时,称为 EBGP(External BGP)。

5.3.1 BGP 的路由属性

BGP 具有源(ORIGIN)属性、AS 路径(AS_PATH)属性、下一跳(NEXT_HOP)属

性、MED(Multi-Exit Discriminator,多出口区分)属性、团体(COMMUNITY)属性、本地优先(LOCAL_PREF)属性、扩展团体属性等路由属性。

5.3.2 BGP的配置命令

表5-3所示是配置BGP时所需用到的一些命令。

表5-3 BGP的配置命令

操作命令	操作说明
system-view	进入系统界面
bgp id	创建BGP,并进入BGP配置界面
peer ×.×.×.× as-numberid	创建对等体,并指定对等体的AS号
address-family ipv4	创建BGP IPv4单播地址簇
peer ×.×.×.× enable	使本地路由器与指定对等体交换IPv4单播路由信息的能力

实验3 配置IPv4 BGP

实验目的:掌握IPv4 BGP的配置方法。

实验器材:H3C MSR36-20三台。

实验要求:

(1) R1为AS20,R2、R3为AS10。

(2) R2与R3建立IBGP连接。

(3) 全网路由互通。

IPv4 BGP的配置拓扑图如图5-5所示。

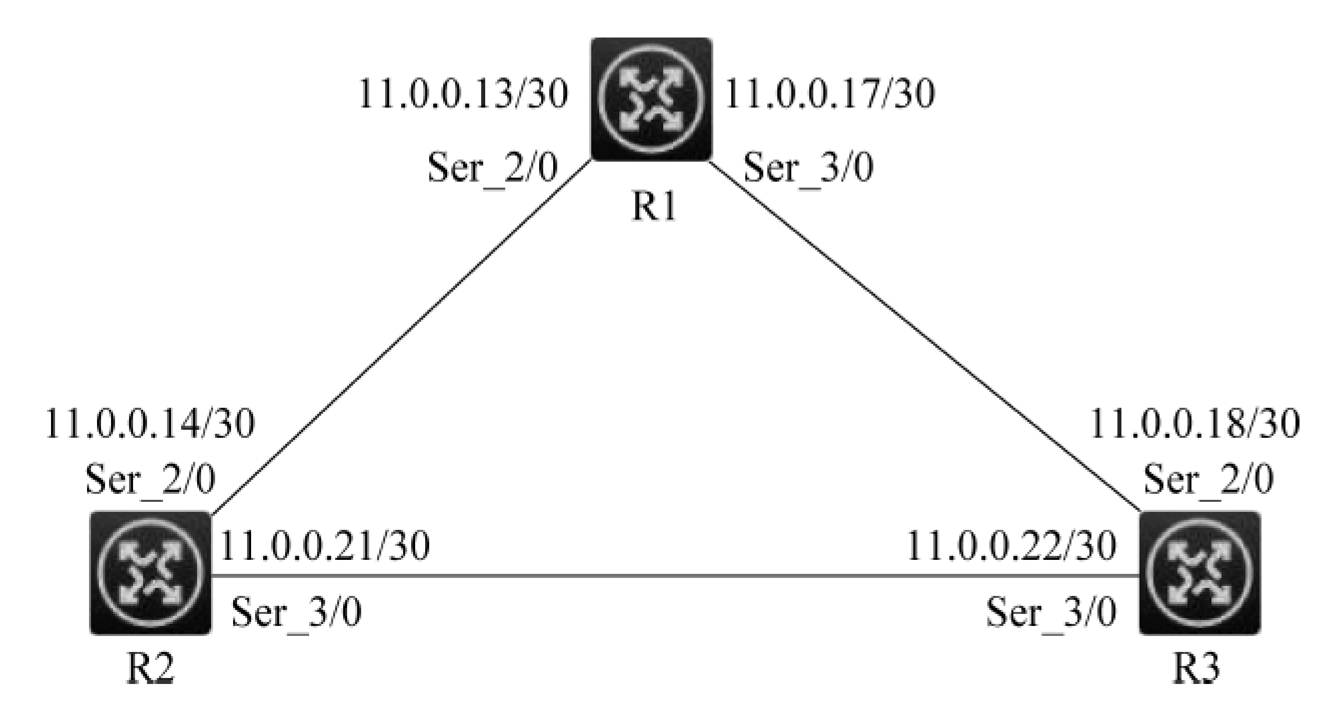


图5-5 IPv4 BGP的配置拓扑图

实验步骤如下:

```
[R1]interface Serial2/0
[R1-Serial2/0]ip address 11.0.0.13 30
```

```
[R1-Serial2/0]quit
[R1]interface Serial3/0
[R1-Serial3/0]ip address 11.0.0.17 30
[R1]bgp 20                                          //设置 AS 号,并接入 BGP 视图
[R1-bgp]peer 11.0.0.14 as-number 10
  //创建 IPv4 BGP 对等体,并指定对等体的 AS 号为 10
[R1-bgp]address-family ipv4
  //创建 BGP IPv4 单播地址簇
[R1-bgp-ipv4]peer 11.0.0.14 enable
  //使本地路由器与指定对等体交换 IPv4 单播路由信息的能力
[R1-bgp-ipv4]quit
[R1-bgp]peer 11.0.0.18 as-number 10
[R1-bgp]address-family ipv4
[R1-bgp-ipv4]peer 11.0.0.18 enable

[R2]interface Serial2/0
[R2-Serial2/0]ip address 11.0.0.14 30
[R2-Serial2/0]quit
[R2]interface Serial 3/0
[R2-Serial3/0]ip address 11.0.0.21 30
[R2]bgp 10
[R2-bgp]peer 11.0.0.13 as-number 20
  //创建 IPv4 BGP 对等体,并指定对等体的 AS 号为 20
[R2-bgp]address-family ipv4
[R2-bgp-ipv4]peer 11.0.0.13 enable
[R2-bgp-ipv4]quit
[R2-bgp]peer 11.0.0.22 as-number 10
[R2-bgp]address-family ipv4
[R2-bgp-ipv4]peer 11.0.0.22 enable

[R3]interface Serial2/0
[R3-Serial2/0]IP address 11.0.0.18 30
[R3-Serial2/0]quit
[R3]interface Serial 3/0
[R3-Serial3/0]ip address 11.0.0.22 30
[R3]bgp 10
[R3-bgp]peer 11.0.0.17 as-number 20
[R3-bgp]address-family ipv4
[R3-bgp-ipv4]peer 11.0.0.17 enable
[R3-bgp-ipv4]quit
[R3-bgp]peer 11.0.0.21 as-number 10
[R3-bgp]address-family ipv4
[R3-bgp-ipv4]peer 11.0.0.21 enable
```

实验结果如下：

```
[R1]display bgp peer ipv4
BGP local router ID: 11.0.0.17
```

```
Local AS number: 20
Total number of peers: 2                  Peers in established state: 2
 * - Dynamically created peer
Peer        AS   MsgRcvd  MsgSent  OutQ   PrefRcv   Up/Down State
11.0.0.14   10      8        9       0     0 00:05:06  Established
11.0.0.18   10      5        5       0     0 00:02:19  Established

[R2]display bgp peer ipv4
BGP local router ID: 11.0.0.21
Local AS number: 10
Total number of peers: 2                  Peers in established state: 2
 * - Dynamically created peer
Peer        AS   MsgRcvd  MsgSent  OutQ   PrefRcv   Up/Down State
11.0.0.13   20     15       13       0     0 00:09:24  Established
11.0.0.22   10      9       10       0     0 00:06:07  Established

[R3]display bgp peer ipv4
BGP local router ID: 11.0.0.22
Local AS number: 10
Total number of peers: 2                  Peers in established state: 2
 * - Dynamically created peer
Peer        AS   MsgRcvd  MsgSent  OutQ   PrefRcv   Up/Down State
11.0.0.17   20      6        6       0     0 00:03:07  Established
11.0.0.21   10      6        5       0     0 00:02:37  Established
```

5.4 RIP 简 介

RIP 是一种基于距离矢量(Distance-Vector)算法的动态路由选择协议,RIP 使用跳数来衡量到达目的地址的距离,跳数称为度量值。范围限制在 15 跳(15 度)之内。华三定义的管理距离(AD,即优先级)是 100。

5.4.1 RIP 两个版本的比较

RIP 有两个版本:RIP-V1 和 RIP-V2。RIP-V1 与 RIP-V2 有以下区别。

(1) RIP-V1 是有类路由协议,RIP-V2 是无类路由协议。

(2) RIP-V1 广播路由更新,RIP-V2 组播路由更新。

(3) RIP-V2 路由更新所携带的信息要比 RIP-V1 多。

5.4.2 RIP 的配置命令

表 5-4 所示是配置 RIP 时所需用到的一些命令。

表 5-4　RIP 的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
rip id	创建 RIP,并进入 RIP 配置界面
undo summary	关闭自动汇总
version number	选择版本
Network ×.×.×.×	发布网段
import-route rip id	引入外部路由

实验 4　配 置 RIP

实验目的：掌握 RIP 的配置方法。

实验器材：MSR36-20 三台、串行线三条。

实验要求：RIP 进程号为 10，版本号为 RIP-V2，取消自动聚合。为管理方便，需发布 Loopback 地址。

实验拓扑：RIP 的配置拓扑图如图 5-6 所示。

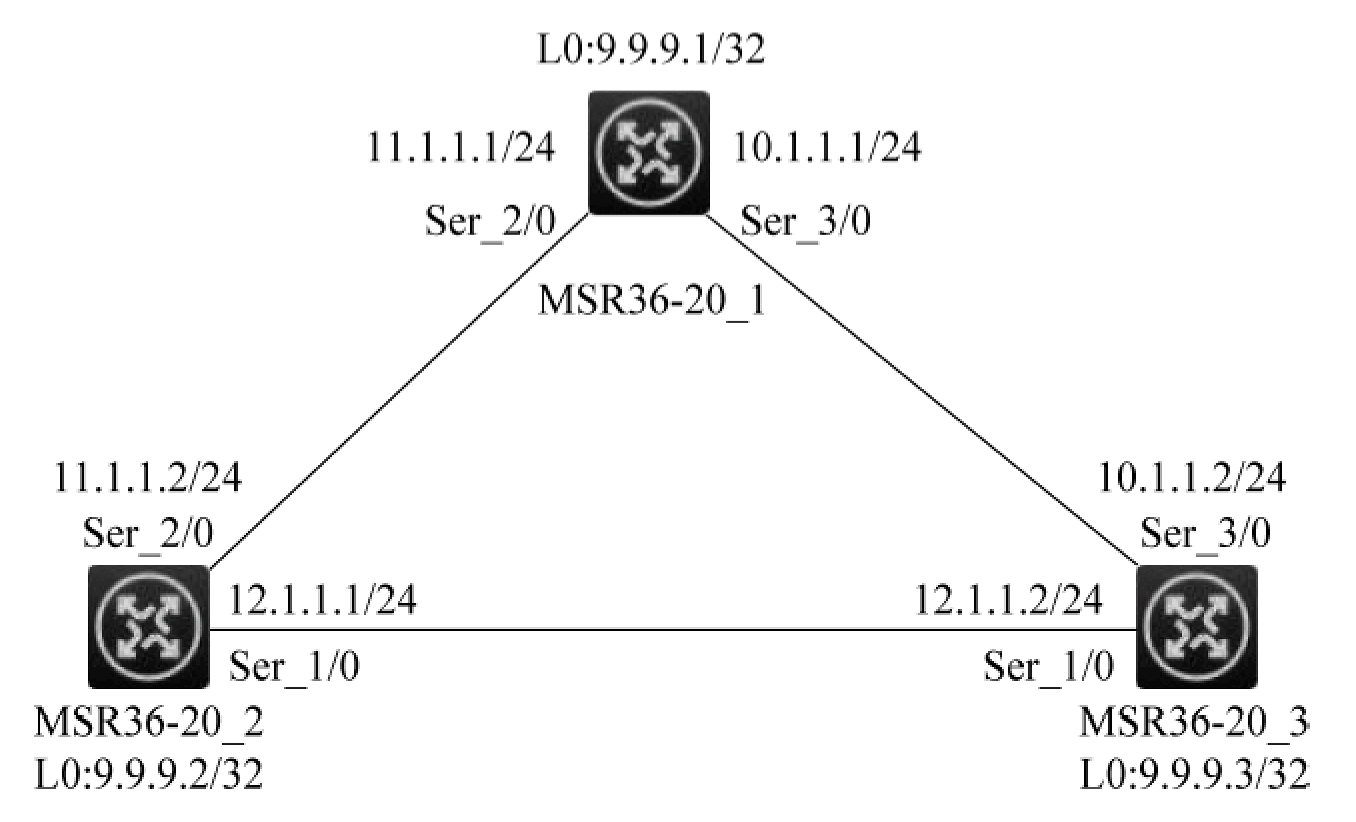


图 5-6　RIP 的配置拓扑图

实验步骤如下：

```
[R1]interface Serial 2/0
[R1-Serial2/0]ip address 11.1.1.1 24
[R1]interface Serial 3/0
[R1-Serial3/0]ip address 10.1.1.1 24
[R1]interface LoopBack 0                  //进入环回地址
[R1-LoopBack0]ip address 9.9.9.1 32
[R1]rip 5                                 //设置 RIP 的进程号为 5
[R1-rip-5]undo summary                    //关闭自动汇总
[R1-rip-5]version 2                       //设置版本
[R1-rip-5]network 11.1.1.1                //发布网段
```

```
[R1-rip-5]network 10.1.1.1
[R1-rip-5]network 9.9.9.1

[R2]int Serial 2/0
[R2-Serial2/0]ip address 11.1.1.2 24
[R2]interface Serial 1/0
[R2-Serial1/0]ip address 12.1.1.1 24
[R2]interface LoopBack 0
[R2-LoopBack0]ip address 9.9.9.2 32
[R2]rip 5
[R2-rip-5]undo summary
[R2-rip-5]version 2
[R2-rip-5]network 11.1.1.2
[R2-rip-5]network 12.1.1.1
[R2-rip-5]network 9.9.9.2
[R3]int Serial 1/0
[R3-Serial1/0]ip address 12.1.1.2 24
[R3-Serial1/0]quit
[R3]int Serial 3/0
[R3-Serial3/0]ip address 10.1.1.2 24
[R3]interface LoopBack 0
[R3-LoopBack0]ip address 9.9.9.3 32
[R3]rip 5
[R3-rip-5]undo summary
[R3-rip-5]version 2
[R3-rip-5]network 10.1.1.2
[R3-rip-5]network 12.1.1.2
[R3-rip-5]network 9.9.9.3
```

实验结果如下：

```
[R1]display rip 5 route
Route Flags: R - RIP, T - TRIP
             P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
             D - Direct, O - Optimal, F - Flush to RIB
---------------------------------------------------------Peer 10.1.1.2 on Serial3/0
    Destination/Mask   Nexthop   Cost  Tag  Flags  Sec
    12.1.1.0/24        10.1.1.2   1     0    RAOF   14
    9.9.9.3/32         10.1.1.2   1     0    RAOF   14
Peer 11.1.1.2 on Serial2/0
    Destination/Mask   Nexthop   Cost  Tag  Flags  Sec
    12.1.1.0/24        11.1.1.2   1     0    RAOF   28
    9.9.9.2/32         11.1.1.2   1     0    RAOF   28
Local route
    Destination/Mask   Nexthop   Cost  Tag  Flags  Sec
    11.1.1.0/24        0.0.0.0    0     0    RDOF   -
    10.1.1.0/24        0.0.0.0    0     0    RDOF   -
    9.9.9.1/32         0.0.0.0    0     0    RDOF   -
```

```
[R2]display rip 5 route
Route Flags: R - RIP, T - TRIP
             P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
             D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------Peer 11.1.1.1 on Serial2/0
    Destination/Mask   Nexthop   Cost   Tag   Flags   Sec
    10.1.1.0/24        11.1.1.1   1      0    RAOF    16
    9.9.9.1/32         11.1.1.1   1      0    RAOF    16
Peer 12.1.1.2 on Serial1/0
    Destination/Mask   Nexthop   Cost   Tag   Flags   Sec
    10.1.1.0/24        12.1.1.2   1      0    RAOF    21
    9.9.9.3/32         12.1.1.2   1      0    RAOF    21
Local route
    Destination/Mask   Nexthop   Cost   Tag   Flags   Sec
    11.1.1.0/24        0.0.0.0    0      0    RDOF    -
    12.1.1.0/24        0.0.0.0    0      0    RDOF    -
    9.9.9.2/32         0.0.0.0    0      0    RDOF    -
[R3]display rip 5 route
Route Flags: R - RIP, T - TRIP
             P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
             D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------Peer 10.1.1.1 on Serial3/0
    Destination/Mask   Nexthop   Cost   Tag   Flags   Sec
    11.1.1.0/24        10.1.1.1   1      0    RAOF    26
    9.9.9.1/32         10.1.1.1   1      0    RAOF    26
Peer 12.1.1.1 on Serial1/0
    Destination/Mask   Nexthop   Cost   Tag   Flags   Sec
    11.1.1.0/24        12.1.1.1   1      0    RAOF    8
    9.9.9.2/32         12.1.1.1   1      0    RAOF    8
Local route
    Destination/Mask   Nexthop   Cost   Tag   Flags   Sec
    10.1.1.0/24        0.0.0.0    0      0    RDOF    -
    12.1.1.0/24        0.0.0.0    0      0    RDOF    -
    9.9.9.3/32         0.0.0.0    0      0    RDOF    -
```

实验 5　配置 RIP 并引入外部路由

实验目的：学会如何引入外部路由。

实验器材：H3C MSR36-20 三台。

实验要求：

(1) 在 R2 上运行 RIP 10 和 RIP 20。

(2) R2 通过 RIP 10 和 R1 交换路由信息，通过 RIP 20 和 R3 交换路由信息。在 R2 上配置 RIP 进程 20 并引入外部路由，引入直连路由和 RIP 进程 100 的路由，

使得 R3 能够学习到达 11.0.0.1/24 的路由，但 R1 不能学习到达 12.1.1.2/24 的路由。

实验拓扑：外部路由引入拓扑图如图 5-7 所示。

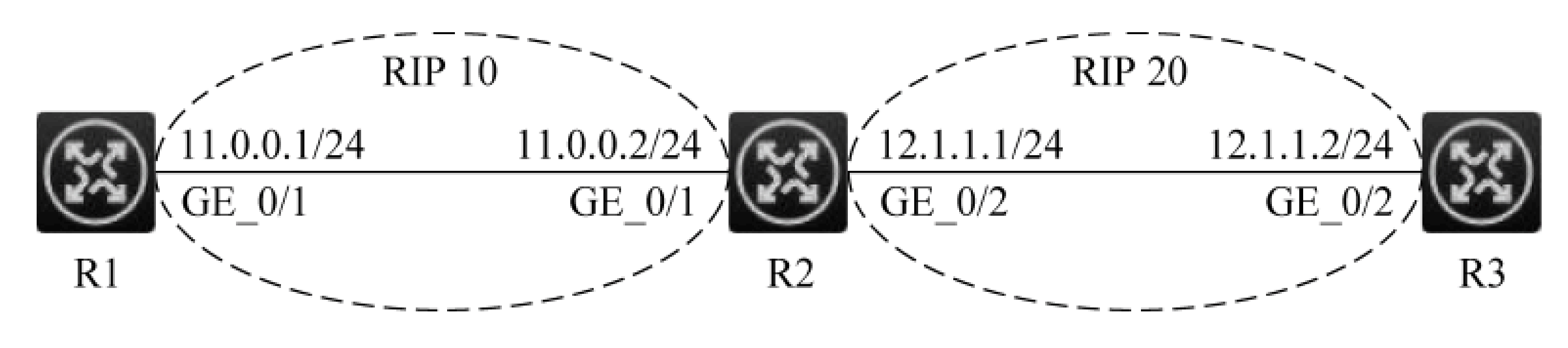


图 5-7　外部路由引入拓扑图

实验步骤如下：

```
[R1]interface GigabitEthernet 0/1
[R1-GigabitEthernet0/1]ip add 11.0.0.1 24
[R1]RIP 10
[R1-rip-10]network 11.0.0.0
[R1-rip-10]version 2
[R1-rip-10]undo summary

[R2]interface GigabitEthernet 0/1
[R2-GigabitEthernet0/1]ip add 11.0.0.2 24
[R2-GigabitEthernet0/1]quit
[R2]interface GigabitEthernet 0/2
[R2-GigabitEthernet0/2]ip add 12.1.1.1 24

[R2]rip 10
[R2-rip-10]network 11.0.0.0
[R2-rip-10]version 2
[R2-rip-10]undo summary
[R2-rip-10]quit
[R2]rip 20
[R2-rip-20]network 12.0.0.0
[R2-rip-20]version 2
[R2-rip-20]undo summary
[R2-rip-20]quit

[R3]interface GigabitEthernet 0/2
[R3-GigabitEthernet0/2]ip add 12.1.1.2 24
[R2]rip 20
[R2-rip-20]network 12.0.0.0
[R2-rip-20]version 2
[R2-rip-20]undo summary
```

现在查看未引入外部路由时 R3 的路由表信息。

```
[R3]display ip routing-table
Destinations : 12 Routes : 12
```

```
Destination/Mask     Proto   Pre  Cost   NextHop      Interface
0.0.0.0/32           Direct  0    0      127.0.0.1    InLoop0
12.1.1.0/24          Direct  0    0      12.1.1.2     GE0/2
12.1.1.0/32          Direct  0    0      12.1.1.2     GE0/2
12.1.1.2/32          Direct  0    0      127.0.0.1    InLoop0
12.1.1.255/32        Direct  0    0      12.1.1.2     GE0/2
127.0.0.0/8          Direct  0    0      127.0.0.1    InLoop0
127.0.0.0/32         Direct  0    0      127.0.0.1    InLoop0
127.0.0.1/32         Direct  0    0      127.0.0.1    InLoop0
127.255.255.255/32   Direct  0    0      127.0.0.1    InLoop0
224.0.0.0/4          Direct  0    0      0.0.0.0      NULL0
255.255.255.255/32   Direct  0    0      127.0.0.1    InLoop0
```

下面在 R2 上配置 RIP 并引入外部路由。

```
[R2]rip 20
[R2-rip-20]import-route rip 10
[R2-rip-20]import-route direct
```

实验结果如下：

```
[R3]display ip routing-table
Destinations : 13Routes : 13

Destination/Mask     Proto   Pre  Cost   NextHop      Interface
0.0.0.0/32           Direct  0    0      127.0.0.1    InLoop0
11.0.0.0/24          RIP     100  1      12.1.1.1     GE0/2
12.1.1.0/24          Direct  0    0      12.1.1.2     GE0/2
12.1.1.0/32          Direct  0    0      12.1.1.2     GE0/2
12.1.1.2/32          Direct  0    0      127.0.0.1    InLoop0
12.1.1.255/32        Direct  0    0      12.1.1.2     GE0/2
127.0.0.0/8          Direct  0    0      127.0.0.1    InLoop0
127.0.0.0/32         Direct  0    0      127.0.0.1    InLoop0
127.0.0.1/32         Direct  0    0      127.0.0.1    InLoop0
127.255.255.255/32   Direct  0    0      127.0.0.1    InLoop0
224.0.0.0/24         Direct  0    0      0.0.0.0      NULL0
255.255.255.255/32   Direct  0    0      127.0.0.1    InLoop0
```

5.5 OSPF 简介

OSPF(Open Shortest Path First，开放式最短路径优先)是 IETF(Internet Engineering Task Force，互联网工程任务组)组织开发的一个基于链路状态的内部网关协议(Interior Gateway Protocol，IGP)。

5.5.1 OSPF 的区域

为了解决在网络规模增大后造成的网络中大量的 OSPF 协议报文传递，从而降低了

网络的带宽利用率。OSPF 协议通过自治系统划分成不同区域来解决这一问题。

OSPF 区域大致可分为骨干区域、Stub 区域、Totally Stub 区域、NSSA 区域和 Totally NSSA 区域。

5.5.2 OSPF 路由器类型

OSPF 路由器根据在 AS 中的不同位置，分为区域内路由器、区域边界路由器 ABR、骨干路由器、自治系统边界路由器 ASBR 四类。

5.5.3 OSPF 的配置命令

表 5-5 所示是配置 OSPF 时所需用到的一些命令。

表 5-5 OSPF 的配置命令

操作命令	操作说明
system-view	进入系统界面
ospf id	创建 OSPF，并进入配置界面
area id	创建 OSPF 区域
network ×.×.×.×	发布网段
vlink-pee ×.×.×.×	创建虚连接

实验 6 配置简单的 OSPF

实验目的：学会如何配置 OSPF 协议。

实验器材：MSR36-20 三台、串行线三条。

实验要求：OSPF 的进程号为 10，区域为 0，为管理方便，需发布 Loopback 地址。

实验拓扑：配置 OSPF 协议拓扑图如图 5-8 所示。

实验步骤如下：

```
[R1]interface Serial 2/0
[R1-Serial2/0]ip address 11.1.1.1 24
[R1]interface Serial 3/0
[R1-Serial3/0]ip address 10.1.1.1 24
[R1]interface LoopBack 0                          //进入环回地址
[R1-LoopBack0]ip address 9.9.9.1 32
[R1]ospf 10
[R1-ospf-10]area
[R1-ospf-10]area 0
[R1-ospf-10-area-0.0.0.0]network 11.1.1.1 0.0.0.255          //发布网段
```

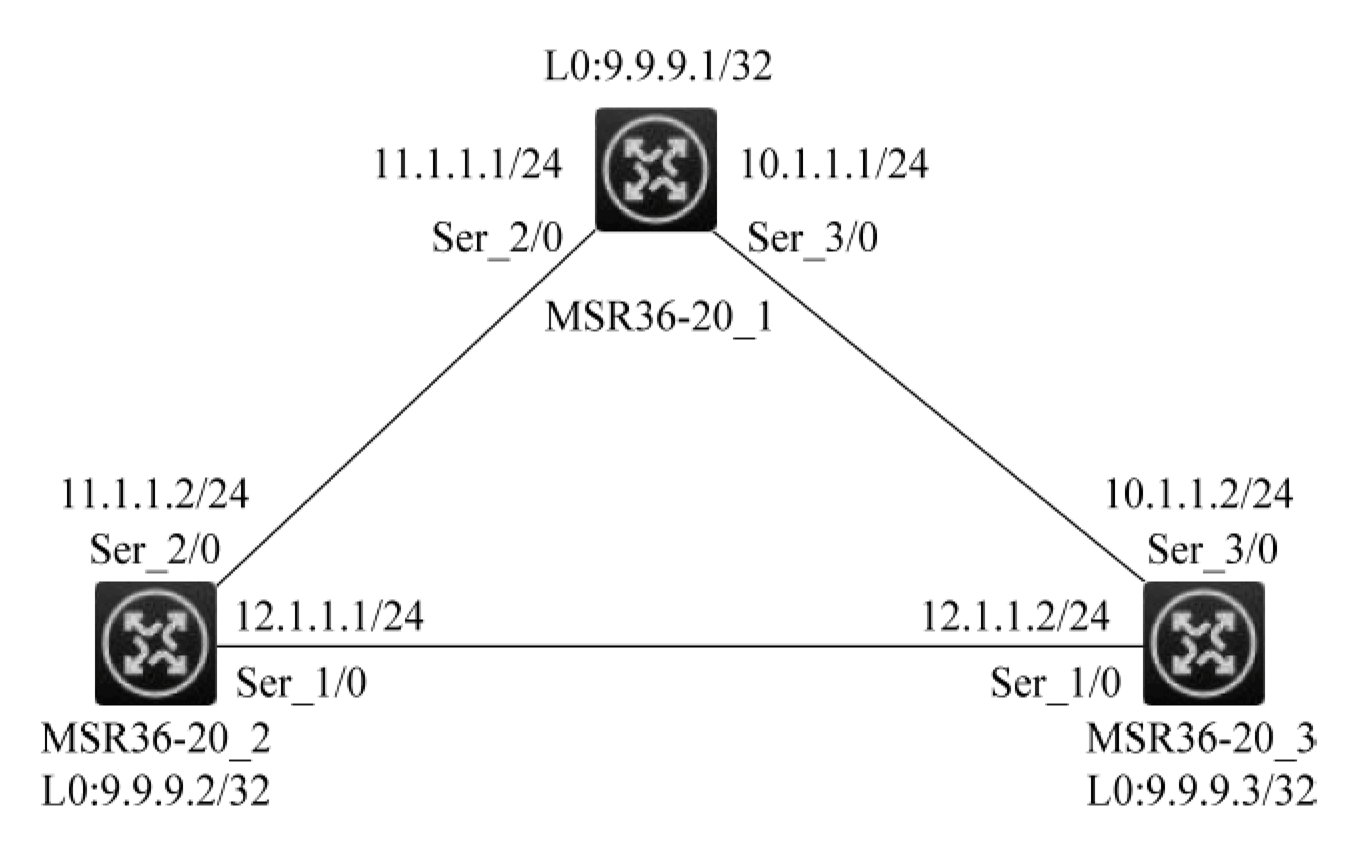


图 5-8 配置 OSPF 协议拓扑图

```
[R1-ospf-10-area-0.0.0.0]network 10.1.1.1 0.0.0.255
[R1-ospf-10-area-0.0.0.0]network 9.9.9.1 0.0.0.0
[R2]int Serial 2/0
[R2-Serial2/0]ip address 11.1.1.2 24
[R2]interface Serial 1/0
[R2-Serial1/0]ip address 12.1.1.1 24
[R2]interface LoopBack 0
[R2-LoopBack0]ip address 9.9.9.2 32
[R2]ospf 10
[R2-ospf-10]area 0
[R2-ospf-10-area-0.0.0.0]network 11.1.1.2 0.0.0.255
[R2-ospf-10-area-0.0.0.0]network 12.1.1.1 0.0.0.255
[R2-ospf-10-area-0.0.0.0]network 9.9.9.2 0.0.0.0

[R3]int Serial 1/0
[R3-Serial1/0]ip address 12.1.1.2 24
[R3-Serial1/0]quit
[R3]int Serial 3/0
[R3-Serial3/0]ip address 10.1.1.2 24
[R3]interface LoopBack 0
[R3-LoopBack0]ip address 9.9.9.3 32
[R3]ospf 10
[R3-ospf-10]area 0
[R3-ospf-10-area-0.0.0.0]network 10.1.1.2 0.0.0.255
[R3-ospf-10-area-0.0.0.0]network 12.1.1.2 0.0.0.255
[R3-ospf-10-area-0.0.0.0]network 9.9.9.3 0.0.0.0
```

实验结果如下：

```
[R1]display ospf peer verbose                //查看 OSPF 的邻居

OSPF Process 10 with Router ID 9.9.9.1 Neighbors
Area 0.0.0.0 interface 11.1.1.1(Serial2/0)'s neighbors
Router ID: 9.9.9.2
Address: 11.1.1.2
```

```
    GR state: Normal
    State: Full
    Mode: Nbr is master
    Priority: 1
    DR: None
    BDR: None
    MTU: 0
    Options is 0x42 (-|O|-|-|-|-|E|-) Dead
    timer due in 35 sec
    Neighbor is up for 00:01:33
    Authentication sequence: [0]
    Neighbor state change count: 5
    BFD status: Disabled

Area 0.0.0.0 interface 10.1.1.1(Serial3/0)'s neighbors
Router ID: 9.9.9.3 Address: 10.1.1.2
    GR state: Normal
    State: Full
    Mode: Nbr is master
    Priority: 1
    DR: None
    BDR: None
    MTU: 0
    Options is 0x42 (-|O|-|-|-|-|E|-) Dead
    timer due in 33 sec
    Neighbor is up for 00:01:12
    Authentication sequence: [0]
    Neighbor state change count: 5
    BFD status: Disabled
[R2]display ospf peer verbose

OSPF Process 10 with Router ID 9.9.9.2 Neighbors

Area 0.0.0.0 interface 12.1.1.1(Serial1/0)'s neighbors
Router ID: 9.9.9.3 Address: 12.1.1.2
    GR state: Normal
    State: Full
    Mode: Nbr is master
    Priority: 1
    DR: None
    BDR: None
    MTU: 0
    Options is 0x42 (-|O|-|-|-|-|E|-) Dead
    timer due in 35 sec
    Neighbor is up for 00:25:51
    Authentication sequence: [0]
    Neighbor state change count: 5
    BFD status: Disabled
```

```
Area 0.0.0.0 interface 11.1.1.2(Serial2/0)'s neighbors
Router ID: 9.9.9.1Address: 11.1.1.1
    GR state: Normal
    State: Full
    Mode: Nbr is slave
    Priority: 1
    DR: None
    BDR: None
    MTU: 0
    Options is 0x42 (-|O|-|-|-|-|E|-) Dead
    timer due in 36 sec
    Neighbor is up for 00:01:57
    Authentication sequence: [0]
    Neighbor state change count: 5
    BFD status: Disabled

[R3]display ospf peer verbose
OSPF Process 10 with Router ID 9.9.9.3 Neighbors

Area 0.0.0.0 interface 12.1.1.2(Serial1/0)'s neighbors
Router ID: 9.9.9.2Address: 12.1.1.1
    GR state: Normal
    State: Full
    Mode: Nbr is slave
    Priority: 1
    DR: None
    BDR: None
    MTU: 0
    Options is 0x42 (-|O|-|-|-|-|E|-) Dead
    timer due in 32 sec
    Neighbor is up for 00:27:19
    Authentication sequence: [0]
    Neighbor state change count: 5
    BFD status: Disabled

Area 0.0.0.0 interface 10.1.1.2(Serial3/0)'s neighbors
Router ID: 9.9.9.1Address: 10.1.1.1
    GR state: Normal
    State: Full
    Mode: Nbr is slave Priority: 1
    DR: None BDR: None MTU: 0
    Options is 0x42 (-|O|-|-|-|-|E|-) Dead
    timer due in 34 sec
    Neighbor is up for 00:02:56
    Authentication sequence: [0]
    Neighbor state change count: 5
    BFD status: Disabled
```

实验 7　配置 OSPF 的虚连接

实验目的：掌握虚连接的配置方法。

实验器材：H3C MSR36-20 四台。

实验要求：

（1）Area2 没有与 Area0 直接相连。

（2）Area1 被用作传输区域(Transit Area)来连接 Area2 和 Area0。

（3）R2 和 R3 之间配置一条虚连接。

虚连接的配置拓扑图如图 5-9 所示。

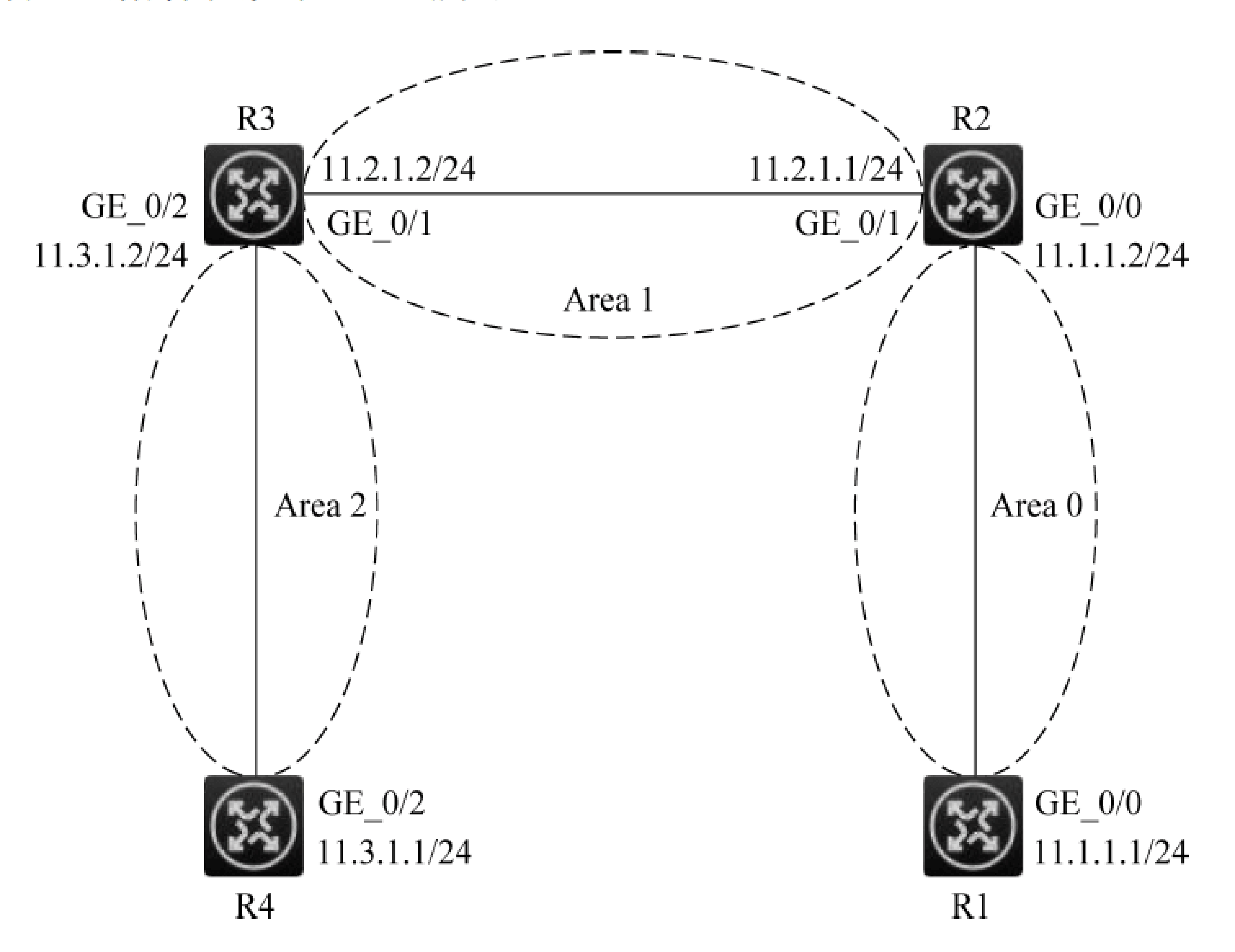


图 5-9　虚连接的配置拓扑图

实验步骤如下：

```
[R1]interface GigabitEthernet 0/0
[R1-GigabitEthernet0/0]ip address 11.1.1.1 24
[Router1] ospf 1 router-id 1.1.1.1
[R1-ospf-1] area 0
[R1-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255

[R2]interface GigabitEthernet 0/0
[R2-GigabitEthernet0/0]ip address 11.1.1.2 24
[R2-GigabitEthernet0/0]quit
[R2]interface GigabitEthernet 0/1
[R2-GigabitEthernet0/1]ip address 11.2.1.1 24
[R2] ospf 1 router-id 2.2.2.2
[R2-ospf-1] area 0
[R2-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
```

```
[R2-ospf-1-area-0.0.0.0] quit
[R2-ospf-1] area 1
[R2-ospf-1-area-0.0.0.1] network 11.2.1.0 0.0.0.255
[R2-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3
[R2-ospf-1-area-0.0.0.1] quit

[R3]interface GigabitEthernet 0/1
[R3-GigabitEthernet0/1]ip address 11.2.1.2 24
[R3-GigabitEthernet0/1]quit
[R3]interface GigabitEthernet 0/2
[R3-GigabitEthernet0/2]ip address 11.3.1.2 24
[R3] ospf 1 router-id 3.3.3.3
[R3-ospf-1] area 1
[R3-ospf-1-area-0.0.0.1] network 11.2.1.0 0.0.0.255
[R3-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[R3-ospf-1-area-0.0.0.1] quit
[R3-ospf-1] area 2
[R3-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[R3-ospf-1-area-0.0.0.2] quit

[R4]interface GigabitEthernet 0/2
[R4-GigabitEthernet0/2]ip address 11.3.1.1 24
[R4] ospf 1 router-id 4.4.4.4
[R4-ospf-1] area 2
[R4-ospf-1-area-0.0.0.2] network 11.3.1.0 0.0.0.255
[R4-ospf-1-area-0.0.0.2] quit
```

实验结果如下：

```
[R1]display ospf routing
OSPF Process 1 with Router ID 1.1.1.1
Routing Table
Topology base (MTID 0)
Routing for network
Destination    Cost    Type       NextHop     AdvRouter     Area
11.1.1.0/24     1      Transit    0.0.0.0      1.1.1.1      0.0.0.0
11.2.1.0/24     2      Inter      11.1.1.2     2.2.2.2      0.0.0.0
11.3.1.0/24     3      Inter      11.1.1.2     3.3.3.3      0.0.0.0

Total nets: 3
Intra area: 1
Inter area: 2
ASE: 0
NSSA: 0
[R2]display ospf routing
OSPF Process 1 with Router ID 2.2.2.2
Routing Table
Topology base (MTID 0)
Routing for network
```

```
Destination      Cost     Type        NextHop      AdvRouter      Area
11.1.1.0/24       1       Transit     0.0.0.0       1.1.1.1       0.0.0.0
11.2.1.0/24       1       Transit     0.0.0.0       2.2.2.2       0.0.0.1
11.3.1.0/24       2       Inter       11.2.1.2      3.3.3.3       0.0.0.0

Total nets: 3
Intra area: 2
Inter area: 1
ASE: 0
NSSA: 0
[R3]display ospf routing
OSPF Process 1 with Router ID 3.3.3.3
Routing Table
Topology base (MTID 0)
Routing for network
Destination      Cost     Type        NextHop      AdvRouter      Area
11.1.1.0/24       2       Transit     11.2.1.1      2.2.2.2       0.0.0.0
11.2.1.0/24       1       Transit     0.0.0.0       2.2.2.2       0.0.0.1
11.3.1.0/24       1       Transit     0.0.0.0       3.3.3.3       0.0.0.2
Total nets: 3
Intra area: 3
Inter area: 0
ASE: 0
NSSA: 0
[R4]display ospf routing
OSPF Process 1 with Router ID 4.4.4.4
Routing Table
Topology base (MTID 0)
Routing for network
Destination      Cost     Type        NextHop      AdvRouter      Area
11.1.1.0/24       3       Inter       11.3.1.2      3.3.3.3       0.0.0.2
11.2.1.0/24       2       Inter       11.3.1.2      3.3.3.3       0.0.0.2
11.3.1.0/24       1       Transit     0.0.0.0       3.3.3.3       0.0.0.2

Total nets: 3
Intra area: 1
Inter area: 2
ASE: 0
NSSA: 0
```

项目 6　三层网络技术

6.1　网络地址转换简介

网络地址转换(Network Address Translation,NAT)是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程。目的是通过使用少量公有 IP 地址来表示众多私有 IP 地址,减少公有 IP 地址的使用。

6.1.1　网络地址转换的类型

网络地址转换的类型可分为静态 NAT、动态 NAT 和端口多路复用。

(1) 静态 NAT:是指将内部网络的私有 IP 地址和公有 IP 地址进行一对一的映射。使用静态 NAT,可以实现内部网络对外部网络的访问。

(2) 动态 NAT:能将未注册的 IP 地址映射到注册 IP 地址池中的地址,但这样映射的 IP 地址是随机、不确定的。动态 NAT 可以使用多个合法的外部地址集。

(3) 端口多路复用:适合利用源端口将多个未注册 IP 地址映射到一个注册 IP 地址,也就是说,内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问,从而可以最大限度地节约 IP 地址资源。

6.1.2　什么情况下使用 NAT

- 当公网不够 IP 用时。
- 当换了 ISP 时,由于网络大而不易改 IP,所以暂时用 NAT 上网。
- 当两个网络有相同地址时,对 TCP 流量做负载均衡。
- 为避免来自 Internet 的攻击,隐藏网络内部的所有主机。

6.1.3　NAT 的配置命令

表 6-1 所示是配置 NAT 时所需用到的一些命令。

表 6-1　NAT 的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
nat static outbound ×.×.×.× ×.×.×.×	配置一对一静态地址转换映射
nat static enable	开启静态 NAT
nat address-group	创建一个 NAT 地址组，并进入 NAT 地址组视图
address	添加地址组成员
natmapping-behavior endpoint-independent	配置 PAT 方式地址转换的模式

实验 1　配置静态 NAT

实验目的：掌握静态 NAT 的配置方法。

实验器材：PC 一台、H3C MSR36-20 一台、外部服务器一台。

实验要求：内部网络用户(IP 地址为 11.110.11.10/24)使用外网地址 202.20.1.101 访问 Internet。

实验拓扑：静态 NAT 的配置拓扑图如图 6-1 所示。

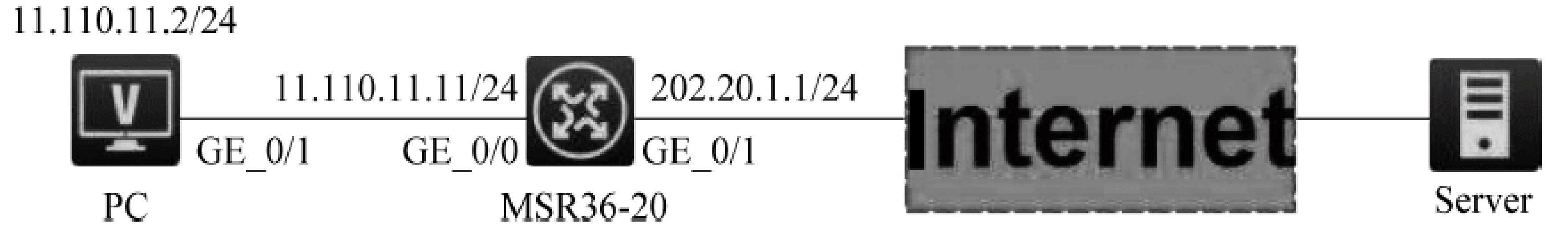


图 6-1　静态 NAT 的配置拓扑图

实验步骤如下：

```
[Router]interface GigabitEthernet 0/0
[Router-GigabitEthernet0/0]ip address 11.110.11.11 24
[Router]interface GigabitEthernet 0/1
[Router-GigabitEthernet0/1]ip address 202.20.1.1 24
[Router]nat static outbound 11.110.11.10 202.20.1.101
//配置内网 IP 地址 11.110.11.10 到外网地址 202.20.1.101 之间的一对一静态地址转换映射
[Router]interface GigabitEthernet 0/1
[Router-GigabitEthernet0/1]nat static enable
//使配置的静态地址转换在 GigabitEthernet 0/1 接口上生效
```

实验结果如下：

```
[Router]display nat
static Static NAT mappings:
Totally 1 outbound static NAT mappings
IP-to-IP:
```

```
Local IP      : 11.110.11.10
Global IP     : 202.20.1.101
Config status: Active
Interfaces enabled with static NAT: Totally 1 interfaces enabled with static NAT
Interface: GigabitEthernet0/1
Config status: Active
```

6.2 IPv6 简 介

IPv6(Internet Protocol Version 6,互联网协议版本 6)是网络层协议的第二代标准协议,也被称为 IPng(IP Next Generation,下一代互联网协议),它是 IETF(Internet Engineering Task Force,互联网工程任务组)设计的一套规范,是 IPv4 的升级版本。IPv6 和 IPv4 之间最显著的区别为 IP 地址的长度从 32 比特增加到 128 比特。

6.2.1 IPv6 协议的特点

IPv6 协议有以下特点。

(1) 简化的报文头格式。通过将 IPv4 报文头中的某些字段裁减或移入扩展报文头,减小了 IPv6 基本报文头的长度。IPv6 使用固定长度的基本报文头,从而简化了转发设备对 IPv6 报文的处理,提高了转发效率。尽管 IPv6 地址长度是 IPv4 地址长度的四倍,但 IPv6 基本报文头的长度只有 40 字节,为 IPv4 报文头长度(不包括选项字段)的两倍。

(2) 充足的地址空间。IPv6 的源地址与目的地址长度都是 128 比特(16 字节)。它可以提供超过 3.4×1038 种可能的地址空间,完全可以满足多层次的地址划分需要,以及公有网络和机构内部私有网络的地址分配。

(3) 层次化的地址结构。IPv6 的地址空间采用了层次化的地址结构,有利于路由快速查找,同时可以借助路由聚合,有效减少 IPv6 路由表占用的系统资源。

(4) 地址自动配置。为了简化主机配置,IPv6 支持有状态地址配置和无状态地址配置:有状态地址配置是指从服务器(如 DHCPv6 服务器)获取 IPv6 地址及相关信息;无状态地址配置是指主机根据自己的数据链路层地址及路由器发布的前缀信息自动配置 IPv6 地址及相关信息。同时,主机也可根据自己的数据链路层地址及默认前缀(FE80::/10)形成链路本地地址,实现与本链路上其他主机的通信。

(5) 内置安全性。IPv6 将 IPSec 作为它的标准扩展头,可以提供端到端的安全特性。这一特性也为解决网络安全问题提供了标准,并提高了不同 IPv6 应用之间的互操作性。

(6) 支持 QoS。IPv6 报文头的流标签(Flow Label)字段实现流量的标识,允许设备对某一流中的报文进行识别并提供特殊处理。

(7) 增强的邻居发现机制。IPv6 的邻居发现协议是通过一组 ICMPv6(Internet Control Message Protocol for IPv6,IPv6 的互联网控制报文协议)消息实现的,管理着邻居节点间(同一链路上的节点)信息的交互。它代替了 ARP(Address Resolution Protocol,地址解析协

议)、ICMPv4 路由器发现和 ICMPv4 重定向消息,并提供了一系列其他功能。

(8) 灵活的扩展报文头。IPv6 取消了 IPv4 报文头中的选项字段,并引入了多种扩展报文头,在提高处理效率的同时还大大增强了 IPv6 的灵活性,为 IP 协议提供了良好的扩展能力。IPv4 报文头中的选项字段最多只有 40 字节,而 IPv6 扩展报文头的大小只受到 IPv6 报文大小的限制。

6.2.2 IPv6 地址

1. IPv6 地址概述

IPv6 地址可以表示为以冒号(:)分隔的一连串 16 比特的十六进制数。每个 IPv6 地址被分为 8 组,每组的 16 比特用 4 个十六进制数表示,组和组之间用冒号隔开,比如:

```
2001:0000:130F:0000:0000:09C0:876A:130B
```

为了简化 IPv6 地址的表示,对于 IPv6 地址中的 0 可以有下面的处理方式:每组中的前导 0 可以省略,即上述地址可写为“2001:0:130F:0:0:9C0:876A:130B”。如果地址中包含一组或连续多组均为 0 的组,则可以用双冒号“::”代替,即上述地址可写为

```
2001:0:130F::9C0:876A:130B
```

IPv6 地址由两部分组成:地址前缀与接口标识。其中,地址前缀相当于 IPv4 地址中的网络号码字段部分;接口标识相当于 IPv4 地址中的主机号码部分。

地址前缀的表示方式为 IPv6 地址/前缀长度。其中,前缀长度是一个十进制数,表示 IPv6 地址最左边多少位为地址前缀。

2. IPv6 地址的分类

IPv6 主要有三种类型的地址:单播地址、组播地址和任播地址。

(1) 单播地址:用来唯一标识一个接口,类似于 IPv4 的单播地址。发送到单播地址的数据报文将被传送给此地址所标识的接口。

(2) 组播地址:用来标识一组接口(通常这组接口属于不同的节点),类似于 IPv4 的组播地址。发送到组播地址的数据报文被传送给此地址所标识的所有接口。

(3) 任播地址:用来标识一组接口(通常这组接口属于不同的节点)。发送到任播地址的数据报文被传送给此地址所标识的一组接口中距离源节点最近(根据使用的路由协议进行度量)的一个接口。IPv6 中没有广播地址,广播地址的功能通过组播地址实现。

3. 单播地址的类型

IPv6 单播地址的类型有多种,包括全球单播地址、链路本地地址等。

(1) 全球单播地址:等同于 IPv4 公网地址,提供给网络服务提供商。这种类型的地址允许路由前缀的聚合,从而限制了全球路由表项的数量。

(2) 链路本地地址:用于邻居发现协议和无状态自动配置中链路本地上节点之间的

通信。使用链路本地地址作为源或目的地址的数据报文不会被转发到其他链路上。

（3）环回地址：单播地址"0:0:0:0:0:0:0:1"（简化表示为"::1"）称为环回地址，不能分配给任何物理接口。它的作用与在 IPv4 中的环回地址相同，即节点用来给自己发送 IPv6 报文。

（4）未指定地址：地址"::"称为未指定地址，不能分配给任何节点。在节点获得有效的 IPv6 地址之前，可在发送的 IPv6 报文的源地址字段填入该地址，但不能作为 IPv6 报文中的目的地址。

4. IEEE EUI-64 格式的接口标识符

IPv6 单播地址中的接口标识符用来标识链路上的一个唯一的接口。目前，IPv6 单播地址基本上都要求接口标识符为 64 位。

不同接口的 IEEE EUI-64 格式的接口标识符的生成方法不同，分别介绍如下。

（1）所有 IEEE 802 接口类型（例如，以太网接口、VLAN 接口）：IEEE EUI-64 格式的接口标识符是从接口的数据链路层地址（MAC 地址）变化而来的。IPv6 地址中的接口标识符是 64 位，而 MAC 地址是 48 位，因此需要在 MAC 地址的中间位置（从高位开始的第 24 位后）插入十六进制数 FFFE（1111111111111110）。为了使接口标识符的作用范围与原 MAC 地址一致，还要将 Universal/Local（U/L）位（从高位开始的第 7 位）进行取反操作。最后得到的这组数就作为 IEEE EUI-64 格式的接口标识符。

（2）Tunnel 接口：IEEE EUI-64 格式的接口标识符的低 32 位为 Tunnel 接口的源 IPv4 地址，ISATAP 隧道的接口标识符的高 32 位为 0000:5EFE，其他隧道的接口标识符的高 32 位为全 0。

（3）其他接口类型（例如，Serial 接口）：IEEE EUI-64 格式的接口标识符由设备随机生成。

6.2.3　IPv6 的配置命令

表 6-2 所示是配置 IPv6 时所需用到的一些命令。

表 6-2　IPv6 的配置命令

操作命令	操作说明
system-view	进入系统界面
int number	进入端口配置界面
ipv6 address ×:×::×:×/m	设置 IPv6 地址
undo ipv6 nd ra halt	允许其发布 RA 消息
ipv6 pathmtu	配置指定 IPv6 地址对应的静态 PMTU 值
ipv6 pathmtu age time	配置 PMTU 老化时间
ipv6 fast-forwarding	IPv6 快速转发

实验 2　配 置 IPv6

实验目的：掌握 IPv6 的配置方法

实验器材：H3C MSR36-20 两台、PC 一台。

实验要求：R2 有可以到 PC 的路由。

在 Host 上安装 IPv6，根据 IPv6 邻居发现协议自动配置 IPv6 地址，有可以到 R2 的路由。

实验拓扑：IPv6 地址的配置拓扑图如图 6-2 所示。

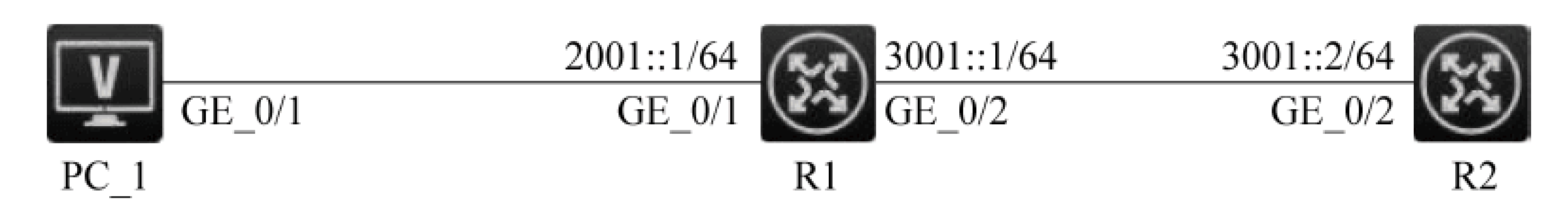


图 6-2　IPv6 地址的配置拓扑图

实验步骤如下：

```
[R1] interface gigabitethernet 0/2
[R1-GigabitEthernet0/2 ipv6 address 3001::1/64      //设置 IPv6 的地址
[R1-GigabitEthernet0/2] quit
[R1] interface gigabitethernet 0/1
[R1-GigabitEthernet0/1] ipv6 address 2001::1/64
[R1-GigabitEthernet0/1] undo ipv6 nd ra halt        //允许其发布 RA 消息
[R1-GigabitEthernet0/1] quit

[R2] interface gigabitethernet 0/2
[R2-GigabitEthernet0/2] ipv6 address 3001::2/64
[R2-GigabitEthernet0/2] quit
[R2] ipv6 route-static 2001:: 64 3001::1
  //配置 IPv6 静态路由，该路由的目的地址为“2001::/64”，下一跳地址为“3001::1”
[R1] display ipv6 neighbors interface gigabitethernet 0/1
Type: S-Static    D-Dynamic    O-Openflow      I-Invalid IPv6
Address           Link Layer   VID Interface   State T Age
FE80::215:E9FF:FEA6:7D14 0015-e9a6-7d14 N/A GE0/1 STALE D 1238
2001::15B:E0EA:3524:E791 0015-e9a6-7d14 N/A GE0/1 STALE D 1248
```

通过上面的信息可以知道，Host 上获得的 IPv6 全球单播地址为“2001::15B:E0EA:3524:E791”。

实验结果如下：

```
[R1] display ipv6 interface gigabitethernet 0/2
GigabitEthernet0/2 current state: UP
Line protocol current state: UP
```

```
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:2
  Global unicast address(es):
      3001::1, subnet is 3001::/64
  Joined group address(es):
      FF02::1
      FF02::2
      FF02::1:FF00:1
      FF02::1:FF00:2
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                25829
  InTooShorts:               0
  InTruncatedPkts:           0
  InHopLimitExceeds:         0
  InBadHeaders:              0
  InBadOptions:              0
  ReasmReqds:                0
  ReasmOKs:                  0
  InFragDrops:               0
  InFragTimeouts:            0
  OutFragFails:              0
  InUnknownProtos:           0
  InDelivers:                47
  OutRequests:               89
  OutForwDatagrams:          48
  InNoRoutes:                0
  InTooBigErrors:            0
  OutFragOKs:                0
  OutFragCreates:            0
  InMcastPkts:               6
  InMcastNotMembers:         25747
  OutMcastPkts:              48
  InAddrErrors: 0
  InDiscards: 0
  OutDiscards: 0
[R1] display ipv6 interface gigabitethernet 0/1
GigabitEthernet0/1 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1C0
  Global unicast address(es):
```

```
      2001::1, subnet is 2001::/64
  Joined group address(es):
      FF02::1
      FF02::2
      FF02::1:FF00:1
      FF02::1:FF00:1C0
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds ND
  router advertisements are sent every 600 seconds ND
  router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                272
  InTooShorts:               0
  InTruncatedPkts:           0
  InHopLimitExceeds:         0
  InBadHeaders:              0
  InBadOptions:              0
  ReasmReqds:                0
  ReasmOKs:                  0
  InFragDrops:               0
  InFragTimeouts:            0
  OutFragFails:              0
  InUnknownProtos:           0
  InDelivers:                159
  OutRequests:               1012
  OutForwDatagrams: 35
  InNoRoutes:                0
  InTooBigErrors:            0
  OutFragOKs:                0
  OutFragCreates:            0
  InMcastPkts:               79
  InMcastNotMembers:         65
  OutMcastPkts:              938
  InAddrErrors:              0
  InDiscards:                0
  OutDiscards:               0
[R2] display ipv6 interface gigabitethernet 0/2
GigabitEthernet0/2 current state: UP
Line protocol current state: UP
```

```
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1234
  Global unicast address(es):
      3001::2, subnet is 3001::/64
  Joined group address(es):
      FF02::1
      FF02::2
      FF02::1:FF00:1
      FF02::1:FF00:1234
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                117
  InTooShorts:               0
  InTruncatedPkts:           0
  InHopLimitExceeds:         0
  InBadHeaders:              0
  InBadOptions:              0
  ReasmReqds:                0
  ReasmOKs:                  0
  InFragDrops:               0
  InFragTimeouts:            0
  OutFragFails:              0
  InUnknownProtos:           0
  InDelivers:                117
  OutRequests:               83
  OutForwDatagrams:          0
  InNoRoutes:                0
  InTooBigErrors:            0
  OutFragOKs:                0
  OutFragCreates:            0
  InMcastPkts:               28
  InMcastNotMembers:         0
  OutMcastPkts:              7
  InAddrErrors:              0
  InDiscards:                0
  OutDiscards:               0
```

用 R2 测试是否可以 ping 通。

```
[R2] ping ipv6 -c 1 3001::1
Ping6(56 data bytes) 3001::2 --> 3001::1, press CTRL_C to break
56 bytes from 3001::1, icmp_seq=0 hlim=64 time=4.404 ms
```

```
--- Ping6 statistics for 3001::1 ---
1 packet(s) transmitted, 1 packet(s) received, 0.0%  packet loss round-
trip min/avg/max/std-dev = 4.404/4.404/4.404/0.000 ms
[RouterB] ping ipv6 -c 1 2001::15B:E0EA:3524:E791
Ping6(56 data bytes) 3001::2 -->2001::15B:E0EA:3524:E791, press CTRL_C to break
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=0 hlim=64 time=5.404 ms

--- Ping6 statistics for 2001::15B:E0EA:3524:E791 ---
1 packet(s) transmitted, 1 packet(s) received, 0.0%  packet loss round-
trip min/avg/max/std-dev = 5.404/5.404/5.404/0.000 ms
```

实验 3　配置 IPv6 快速转发

实验目的：掌握 IPv6 快速转发的配置方法。

实验器材：H3C MSR36-20 三台。

实验要求：在 R2 上实现 IPv6 的快速转发。

实验拓扑：IPv6 快速转发的配置拓扑图如图 6-3 所示。

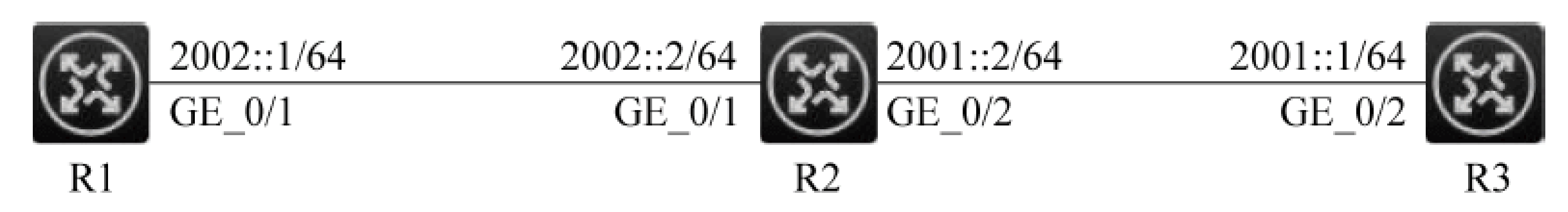


图 6-3　IPv6 快速转发的配置拓扑图

实验步骤如下：

```
[R1] interface gigabitethernet 0/1
[R1-GigabitEthernet0/1] ipv6 address 2002::1 64
[R1-GigabitEthernet2/1/1] quit
[R1] ipv6 route-static 2001:: 64 2002::2              //配置静态路由

[R3] interface gigabitethernet 0/2
[R3-GigabitEthernet0/2] ipv6 address 2001::1 64
[R3-GigabitEthernet0/2] quit
[R3] ipv6 route-static 2002:: 64 2001::2

[R2] ipv6 fast-forwarding                             //开启 IPv6 快速转发功能
[R2] interface gigabitethernet 0/1
[R2-GigabitEthernet0/1] ipv6 address 2002::2 64
[R2-GigabitEthernet0/1] quit
[R2] interface gigabitethernet 0/2
[R2-GigabitEthernet0/2] ipv6 address 2001::2 64
[R2-GigabitEthernet0/2] quit
```

实验结果如下：

```
[R2] display ipv6 fast-forwarding cache
  No IPv6 fast-forwarding entries
  //此时,R2的IPv6快速转发表并未建立

[R1] ping ipv6 2001::1
  PING 2001::1 : 56 data bytes, press CTRL_C to break
    Reply from 2001::1
    bytes=56 Sequence=1 hop limit=64   time =69 ms
    Reply from 2001::1
    bytes=56 Sequence=2 hop limit=64   time =1 ms
    Reply from 2001::1
    bytes=56 Sequence=3 hop limit=64   time =1 ms
    Reply from 2001::1
    bytes=56 Sequence=4 hop limit=64   time =1 ms
    Reply from 2001::1
    bytes=56 Sequence=5 hop limit=64   time =1 ms

    ---2001::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00%  packet loss
round-trip min/avg/max =1/14/69 ms

[R2] display ipv6 fast-forwarding cache
Total number of IPv6 fast-forwarding items: 2
SrcIP: 2002::1
DstIP: 2001::1
Src port: 129
Dst port: 0

Protocol: 58
VPN instance: N/A
Input interface: GE0/1
Output interface: GE0/2
2001::1

DstIP:
2002::1
Src port: 128
Dst port: 0
Protocol: 58
VPN instance: N/A
Input interface: GE0/2
Output interface: GE0/1
  //现在,IPv6快速转发表已建立
```

6.3 路由策略

路由策略是为了改变网络流量所经过的途径而修改路由信息的技术，主要通过改变路由属性（包括可达性）来实现。它是一种比基于目标网络进行路由更加灵活的数据包路由转发机制。应用了路由策略，路由器将通过路由图决定如何对需要路由的数据包进行处理，路由图决定了一个数据包的下一跳转发路由器。路由策略的种类大体上分为两种：一种是根据路由的目的地址来进行的策略，称为目的地址路由；另一种是根据路由源地址来进行策略实施的，称为源地址路由。随着路由策略的发展，现在有了第三种路由方式：智能均衡的策略方式。

6.3.1 路由策略的应用

路由策略的应用灵活广泛，主要有下面几种方式。

（1）控制路由的发布。路由协议在发布路由信息时，通过路由策略对路由信息进行过滤，只发布满足条件的路由信息。

（2）控制路由的接收。路由协议在接收路由信息时，通过路由策略对路由信息进行过滤，只接收满足条件的路由信息。可以控制路由表项的数量，提高网络的安全性。

（3）管理引入的路由。路由协议在引入其他路由协议发现的路由时，通过路由策略只引入满足条件的路由信息，并控制所引入的路由信息的某些属性，以使其满足本协议的要求。

（4）设置路由的属性。对通过路由策略的路由设置相应的属性。

6.3.2 过滤器

过滤器可以看作路由策略过滤路由的工具，单独配置的过滤器没有任何过滤效果，只有在路由协议的相关命令中应用这些过滤器，才能够达到预期的过滤效果。路由协议可以引用访问控制列表、地址前缀列表、AS 路径访问列表、团体属性列表、扩展团体属性列表、MAC 地址列表和路由策略七种过滤器。

1. 访问控制列表

访问控制列表包括针对 IPv4 报文的 ACL 和针对 IPv6 报文的 ACL。用户在定义 ACL 时可以指定 IP(v6)地址和子网范围，用于匹配路由信息的目的网段地址或下一跳地址。

2. 地址前缀列表

地址前缀列表包括 IPv4 地址前缀列表和 IPv6 地址前缀列表。地址前缀列表的作

用类似于 ACL,但比它更为灵活,且更易于用户理解。使用地址前缀列表过滤路由信息时,其匹配对象为路由信息的目的地址信息域;另外,用户可以指定 gateway 选项,指明只接收某些路由器发布的路由信息。一个地址前缀列表由前缀列表名标识。每个前缀列表可以包含多个表项,每个表项可以独立指定一个网络前缀形式的匹配范围,并用一个索引号标识,索引号指明了在地址前缀列表中进行匹配检查的顺序。每个表项之间是“或”的关系,在匹配的过程中,路由器按升序依次检查由索引号标识的各个表项,只要有某一表项满足条件,就意味着通过该地址前缀列表的过滤(不再对下一个表项进行匹配)。

3. AS 路径访问列表(as-path)

as-path 仅用于 BGP 路由的过滤。BGP 的路由信息中,包含有自治系统路径域。as-path 就是针对自治系统路径域指定匹配条件。

4. 团体属性列表(community-list)

community-list 仅用于 BGP 路由的过滤。BGP 的路由信息包中,包含一个 community 属性域,用于标识一个团体。community-list 就是针对团体属性域指定匹配条件。

5. 扩展团体属性列表(extcommunity-list)

extcommunity-list 仅用于 BGP 路由的过滤。BGP 扩展团体属性有两种,一种是用于 VPN 的 RT(Route Target,路由目标)扩展团体;另一种则是 SoO(Site of Origin,源站点)扩展团体。扩展团体属性列表就是针对这两种属性指定匹配条件。

6. MAC 地址列表(mac-list)

mac-list 仅用于 EVI IS-IS。EVI IS-IS 的表项中包含 MAC 地址信息,mac-list 就是针对 MAC 地址信息的匹配条件。一个 MAC 地址列表由 MAC 地址列表名标识。每个 MAC 地址列表可以包含多个表项,每个表项可以独立指定一个 MAC 地址形式的匹配范围,并用一个索引号标识,索引号指明了在 MAC 地址列表中进行匹配检查的顺序。每个表项之间是“或”的关系,匹配过程同前面讲的地址前缀列表。

7. 路由策略

路由策略是一种比较复杂的过滤器,它不仅可以匹配路由信息的某些属性,还可以在条件满足时改变路由信息的属性。路由策略可以使用前面几种过滤器定义自己的匹配规则。一个路由策略可以由多个节点构成,每个节点是匹配检查的一个单元,在匹配过程中,系统按节点序号升序依次检查各个节点。不同节点间是“或”的关系,如果通过了其中一个节点,就意味着通过该路由策略,不再对其他节点进行匹配(配置了 continue 子句的情况除外)。每个节点对路由信息的处理方式由匹配模式决定。匹配模式分为 permit 和 deny 两种。

permit：指定节点的匹配模式为允许模式。当路由信息通过该节点的过滤后，将执行该节点的 apply 子句，不进入下一个节点的匹配(配置了 continue 子句的情况除外)；如果路由信息没有通过该节点过滤，将进入下一个节点继续匹配。

deny：指定节点的匹配模式为拒绝模式(此模式下 apply 子句和 continue 子句不会被执行)。当路由信息通过该节点的过滤后，将被拒绝通过该节点，不进入下一个节点的匹配；如果路由信息没有通过该节点的过滤，将进入下一个节点继续匹配。

每个节点可以由一组 if-match、apply 和 continue 子句组成。

if-match 子句：定义匹配规则，匹配对象是路由信息的一些属性。同一节点中的不同 if-match 子句是"与"的关系，只有满足节点内所有 if-match 子句指定的匹配条件，才能通过该节点的匹配。

apply 子句：指定动作，也就是在通过节点的匹配后，对路由信息的一些属性进行设置。

continue 子句：用来配置下一个执行节点。当路由成功匹配当前路由策略节点(必须是 permit 节点)时，可以指定路由继续匹配同一路由策略内的下一个节点，这样可以组合路由策略各个节点的 if-match 子句和 apply 子句，增强路由策略的灵活性。

if-match、apply 和 continue 子句可以根据应用进行设置，都是可选的。如果只过滤路由，不设置路由的属性，则不需要使用 apply 子句。如果某个 permit 节点没有配置任何 if-match 子句，则该节点匹配所有的路由。通常在多个 deny 节点后设置一个不含 if-match 子句和 apply 子句的 permit 节点，用于允许其他的路由通过。

6.3.3 路由策略的配置命令

表 6-3 所示是配置路由策略时所需用到的一些命令。

表 6-3 路由策略的配置命令

操作命令	操作说明
system-view	进入系统界面
route-policy name { deny | permit } node number	创建路由策略，并进入该路由策略视图
if-match ip ×.×.×.× acl-number |prefix-list	配置 IPv4 路由信息的匹配条件
if-match as-path number	配置 BGP 路由信息的 AS 路径域的匹配条件
apply ip-address next-hop ×.×.×.× [public | vpn-instance name]	配置 IPv4 路由信息的下一跳地址
apply ipv6 next-hop ×:×::×:×/m	配置 IPv6 路由信息的下一跳地址

实验 4 配置 IPv4 路由引入路由策略

实验目的：掌握 IPv4 引入路由策略的配置方法。

实验器材：H3C MSR36-20 三台。

实验要求：R2 与 R1 之间通过 OSPF 协议交换路由信息，与 R3 之间通过 IS-IS 交换路由信息。

在 R2 上配置路由引入，将 IS-IS 路由引入 OSPF 中去，并同时使用路由策略设置路由的属性。其中，设置 172.17.1.0/24 的路由的开销为 100，设置 172.17.2.0/24 的路由的 Tag 属性为 20。

实验拓扑：IPv4 引入路由的配置拓扑图如图 6-4 所示。

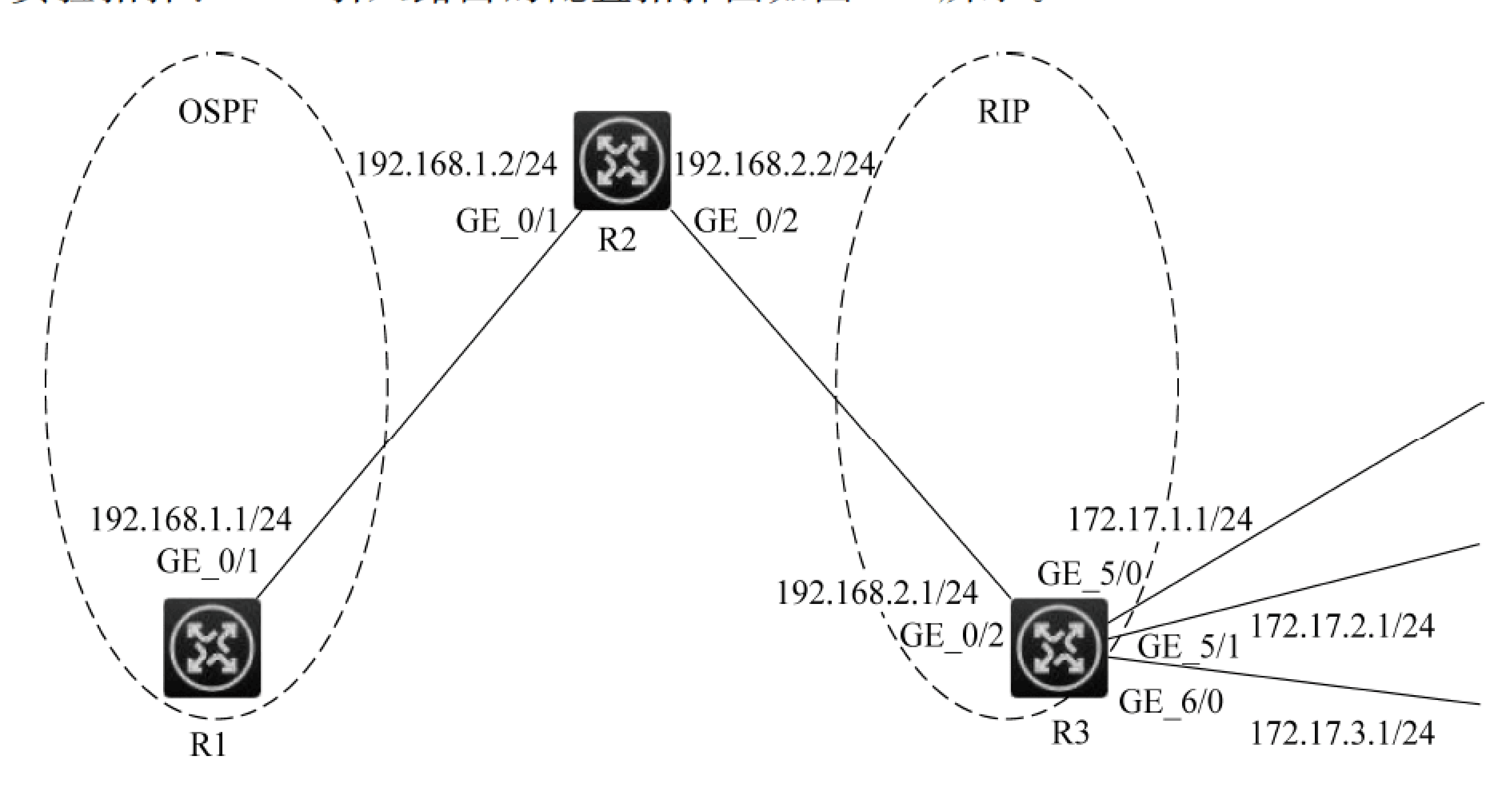


图 6-4　IPv4 引入路由的配置拓扑图

实验步骤如下：

```
[R3]interface GigabitEthernet 0/2
[R3-GigabitEthernet0/2]ip address 192.168.2.1 24
[R3-GigabitEthernet0/2]quit
[R3]interface GigabitEthernet 5/0
[R3-GigabitEthernet5/0]ip address 172.17.1.1 24
[R3-GigabitEthernet5/0]quit
[R3]interface GigabitEthernet 5/1
[R3-GigabitEthernet5/1]ip address 172.17.2.1 24
[R3-GigabitEthernet5/1]quit
[R3]interface GigabitEthernet 6/0
[R3-GigabitEthernet6/0]ip address 172.17.3.1 24
[R3] isis
[R3-isis-1] is-level level-2
[R3-isis-1] network-entity 10.0000.0000.0001.00
[R3-isis-1] quit
[R3] interface gigabitethernet 0/2
[R3-GigabitEthernet0/2] isis enable
[R3-GigabitEthernet0/2] quit
[R3] interface gigabitethernet 5/0
[R3-GigabitEthernet5/0] isis enable
[RouterC-GigabitEthernet5/0] quit
[R3] interface gigabitethernet 5/1
```

```
[R3-GigabitEthernet5/1] isis enable
[R3-GigabitEthernet5/1] quit
[R3] interface gigabitethernet 6/0
[R3-GigabitEthernet6/0] isis enable
[R3-GigabitEthernet6/0] quit

[R1]interface GigabitEthernet 0/1
[R1-GigabitEthernet0/1]ip address 192.168.1.1 24
[R1] ospf
[R1-ospf-1] area 0
[R1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0] quit
[R1-ospf-1] quit
[R2]interface GigabitEthernet 0/1
[R2-GigabitEthernet0/1]ip address 192.168.1.2 24
[R2-GigabitEthernet0/1]quit
[R2]interface GigabitEthernet 0/2
[R2-GigabitEthernet0/2]ip address 192.168.2.2 24
[R2] isis
[R2-isis-1] is-level level-2
[R2-isis-1] network-entity 10.0000.0000.0002.00
[R2-isis-1] quit
[R2] interface gigabitethernet 0/2
[R2-GigabitEthernet/00/2] isis enable
[R2-GigabitEthernet0/2] quit
[R2] ospf
[R2-ospf-1] area 0
[R2-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0] quit
[R2-ospf-1] import-route isis 1              //在 OSPF 中引入 IS-IS 路由
[R2-ospf-1] quit
[R2] acl number 2002                         //创建编号为 2002 的 ACL
[R2-acl-basic-2002] rule permit source 172.17.2.0 0.0.0.255
  //允许 172.17.2.0/24 的路由通过
[R2-acl-basic-2002] quit
[R2] ip prefix-list prefix-a index 10 permit 172.17.1.0 24
  //创建名为 prefix-a 的地址前缀列表,允许 IP 地址为 172.17.1.0 24 的路由通过
[R2] route-policy isis2ospf permit node 10
  //创建路由策略
[R2-route-policy-isis2ospf-10] if-match ip address prefix-list prefix-a
  //配置 IPv4 的路由信息
[R2-route-policy-isis2ospf-10] apply cost 100
  //配置路由信息的开销为 100
[R2-route-policy-isis2ospf-10] quit
[R2] route-policy isis2ospf permit node 20
[R2-route-policy-isis2ospf-20] if-match ip address acl 2002
[R2-route-policy-isis2ospf-20] apply tag 20
```

```
//建立标签为 20

[R2-route-policy-isis2ospf-20] quit
[R2] route-policy isis2ospf permit node 30
[R2-route-policy-isis2ospf-30] quit
[R2] ospf
[R2-ospf-1] import-route isis 1 route-policy isis2ospf
//路由引入时应用路由策略
[R2-ospf-1] quit
```

实验结果如下：

```
[R1] display ospf routing

OSPF Process 1 with Router ID 192.168.1.1
Routing Tables
Routing for Network
Destination     Cost  Type     NextHop      AdvRouter    Area
192.168.1.0/24  1     Transit  192.168.1.1  0.0.0.0      Routing for ASEs
Destination     Cost  Type     Tag          NextHop      AdvRouter
172.17.1.0/24   100   Type2    1            192.168.1.2  192.168.2.2
172.17.2.0/24   1     Type2    20           192.168.1.2  192.168.2.2
172.17.3.0/24   1     Type2    1            192.168.1.2  192.168.2.2
Total Nets: 4
Intra Area: 1     Inter Area: 0     ASE: 3     NSSA: 0
```

实验 5 IPv6 路由引入路由策略配置

实验目的：掌握 IPv6 引入路由策略的配置方法。

实验器材：H3C MSR36-20 两台。

实验要求：

(1) R1 与 R2 通信，都运行 RIPng 协议。

(2) 使能 Router A 上的 RIPng 协议，配置三条静态路由。

(3) 设置在引入静态路由时应用路由策略，使三条静态路由部分引入、部分被屏蔽掉——20::/32 和 40::/32 网段的路由是可见的，30::/32 网段的路由则被屏蔽。

通过在 Router B 上查看 RIPng 路由表，验证路由策略是否生效。

IPv6 引入路由策略的配置拓扑图如图 6-5 所示。

实验步骤如下：

```
[R1] interface gigabitethernet 0/1
[R1-GigabitEthernet0/1] ipv6 address 10::1 32     //配置 IPv6 地址
[R1-GigabitEthernet0/1] quit
[R1] interface gigabitethernet 0/2
[R1-GigabitEthernet0/2] ipv6 address 11::1 32
```

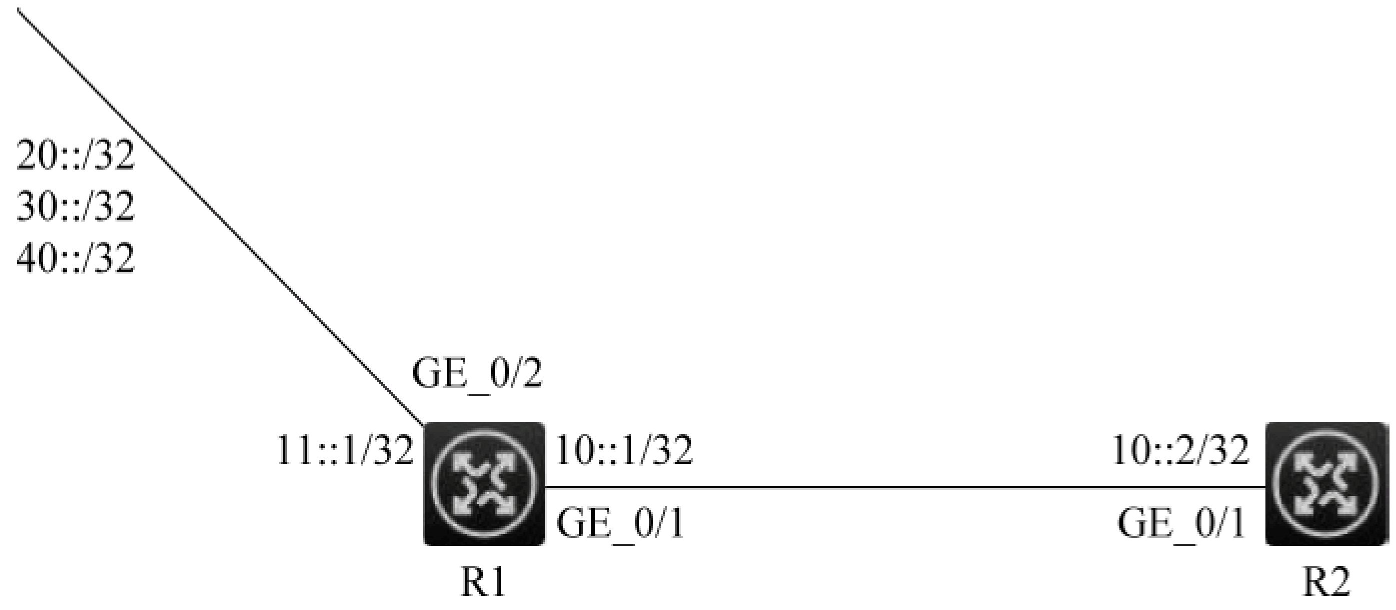


图 6-5　IPv6 引入路由策略的配置拓扑图

```
[R1-GigabitEthernet0/2] quit
[R1] interface gigabitethernet 0/1
[R1-GigabitEthernet0/1] ripng 1 enable              //开启 RIpng
[R1-GigabitEthernet0/1] quit
[R1] ipv6 route-static 20::32 11::2                 //配置静态路由,下一跳为 11::2
[R1] ipv6 route-static 30::32 11::2
[R1] ipv6 route-static 40::32 11::2
[R1] ipv6 prefix-list a index 10 permit 30::32      //配置路由策略
[R1] route-policy static2ripng deny node 0
[R1-route-policy-static2ripng-0] if-match ipv6 address prefix-list a             //匹配
[R1-route-policy-static2ripng-0] quit
[R1] route-policy static2ripng permit node 10
[R1-route-policy-static2ripng-10] quit
[R1] ripng
[R1-ripng-1] import-route static route-policy static2ripng
  //引入名为 static2ripng 的路由策略

[R2] interface gigabitethernet 0/1
[R2-GigabitEthernet0/1] ipv6 address 10::2 32
[R2] ripng
[R2-ripng-1] quit
[R2] interface gigabitethernet 0/1
[R2-GigabitEthernet0/1] ripng 1 enable

[R2-GigabitEthernet0/1] quit
```

实验结果如下：

```
[R2] display ripng 1 route
    Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
-------------------------------------------------------------------
Peer FE80::7D58:0:CA03:1 on GigabitEthernet2/1/1
Destination 10::/32,via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 18 secs
Destination 20::/32,via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 8 secs
Destination 40::/32,via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 3 secs
```

6.4 策略路由简介

策略用来定义报文的匹配规则，以及对报文执行的操作。策略由节点组成。一个策略可以包含一个或者多个节点。节点的构成如下。

每个节点由节点编号标识。节点编号越小，节点的优先级越高，优先级高的节点优先被执行。

每个节点的具体内容由 if-match 子句和 apply 子句指定。if-match 子句定义该节点的匹配规则；apply 子句定义该节点的动作。

每个节点对报文的处理方式由匹配模式决定。匹配模式分为 permit（允许）和 deny（拒绝）两种。应用策略后，系统将根据策略中定义的匹配规则和操作，对报文进行处理：系统按照优先级从高到低的顺序依次匹配各节点，如果报文能满足这个节点的匹配规则，就执行该节点的动作；如果报文不能满足这个节点的匹配规则，就继续匹配下一个节点；如果报文不能满足策略中任何一个节点的匹配规则，则根据路由表转发报文。

6.4.1 if-match 与 apply 子句

1. if-math 子句

目前，策略路由提供了两种 if-match 子句，作用如下。

if-match acl：设置 ACL 匹配规则。

if-match packet-length：设置 IP 报文长度匹配规则。

在一个节点中可以配置多条 if-match 子句，同一类型的 if-match 子句最多只能有一条。同一个节点中的各个 if-match 子句之间是“与”的关系，即报文必须满足该节点的所有 if-match 子句才算满足这个节点的匹配规则。

2. apply 子句

策略路由提供了 12 种 apply 子句，同一个节点中可以配置多条 apply 子句，但配置的多条 apply 子句不一定都会执行。影响报文转发路径的 apply 子句有五条，优先级顺序是 apply access-vpn vpn-instance、apply next-hop、apply output-interface、apply default-next-hop 和 apply default-output-interface。

6.4.2 策略路由的种类

策略路由的种类大体上分为两种：一种是根据路由的目的地址进行策略实施的，称为目的地址路由；另一种是根据路由源地址进行策略实施的，称为源地址路由。随着策略路由的发展，现在有了第三种路由方式：智能均衡的策略方式。

实验 6　配置基于报文协议类型的本地策略路由

实验目的：掌握本地策略路由的配置方法。

实验器材：H3C MSR36-20 一台。

实验要求：

（1）指定所有 TCP 报文的下一跳为 1.1.2.2。

（2）其他报文仍然按照查找路由表的方式进行转发。

本地策略路由的配置拓扑图如图 6-6 所示。

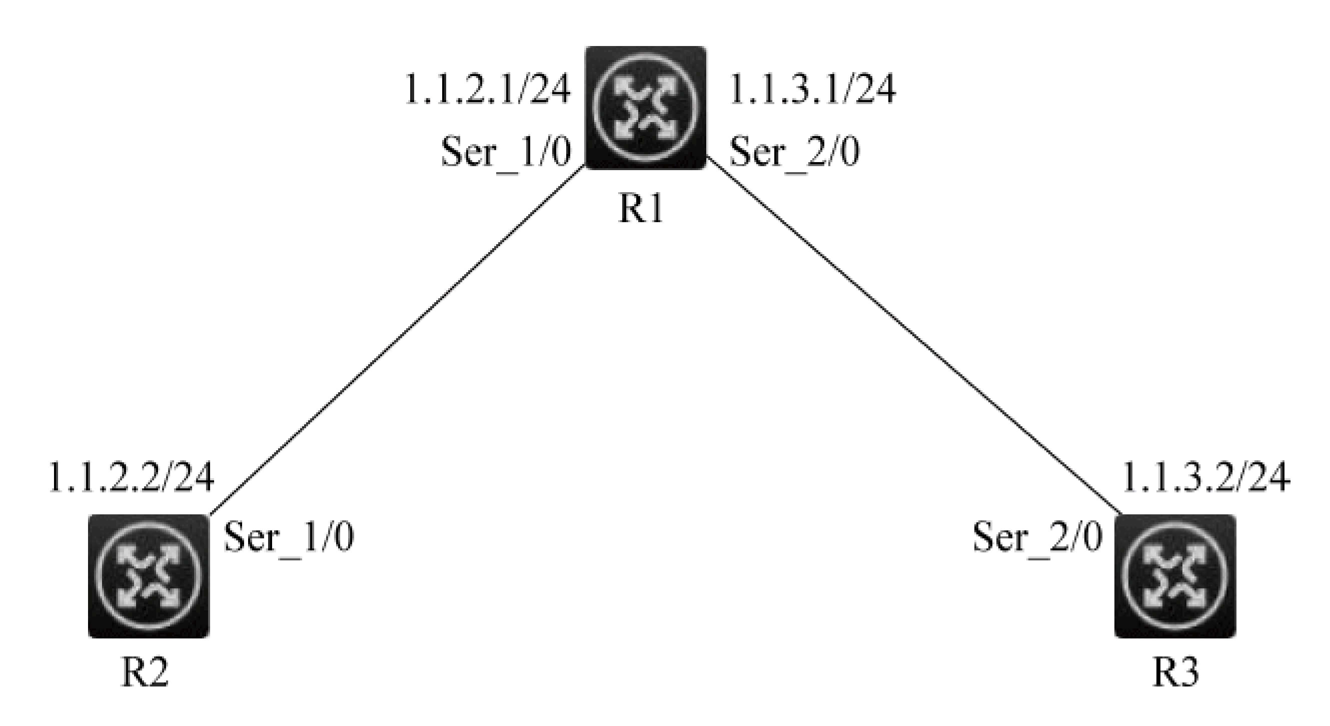


图 6-6　本地策略路由的配置拓扑图

实验步骤如下：

```
[R1] interface serial 1/0
[R1-Serial1/0] ip address 1.1.2.1 24
[R1-Serial1/0] quit
[R1] interface serial 2/0
[R1-Serial2/0] ip address 1.1.3.1 24
[R1-Serial2/0] quit
[R1] acl number 3101
[R1-acl-adv-3101] rule permit tcp          //匹配 TCP
[R1-acl-adv-3101] quit
[R1] policy-based-route aaa permit node 5
  //定义名称为 aaa,节点为 5 的策略路由
[R1-pbr-aaa-5] if-match acl 3101
[R1-pbr-aaa-5] apply next-hop 1.1.2.2
  //设置下一跳地址为 1.1.2.2
[R1-pbr-aaa-5] quit
[R1] ip local policy-based-route aaa
  //在 R1 上应用本地策略路由

<R2> system-view
[R2] interface serial 1/0
[R2-Serial1/0] ip address 1.1.2.2 24
```

```
<R3>system-view
[R3] interface serial 2/0
[R3-Serial2/0] ip address 1.1.3.2 24
```

实验结果如下：

从 R1 上通过 Telnet 方式登录 R2(1.1.2.2/24)，结果成功。从 R1 上通过 Telnet 方式登录 R3(1.1.3.2/24)，结果失败。从 R1 上 ping R3(1.1.3.2/24)，结果成功。

由于 Telnet 使用的是 TCP，ping 使用的是 ICMP，所以由以上结果可证明：R1 产生的 TCP 报文的下一跳为 1.1.2.2，串口 Serial 2/0 不发送 TCP 报文，但可以发送非 TCP 报文，策略路由设置成功。

项目 7　ACL 与 QoS 部署

7.1　ACL 简 介

ACL(Access Control List,访问控制列表)是一条或多条规则的集合,是路由器和交换机接口的指令列表,用来控制端口进出的数据包。

7.1.1　ACL 的分类

目前,主要有三种 ACL,分别是基本 ACL、高级 ACL 和二层 ACL。

(1) 基本 ACL:使用 2000～2999 的编号,可适用于 IPv4 与 IPv6,其作用为可以阻止、允许来自某一网络的所有通信流量。

(2) 高级 ACL:使用 3000～3999 的编号,可适用于 IPv4 与 IPv6,可让网络管理员更好、更简便地管理网络的通信流量。

(3) 二层 ACL:使用 4000～4999 的编号。

7.1.2　ACL 的配置命令

表 7-1 所示是配置 ACL 时所需用到的一些命令。

表 7-1　ACL 的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
acl basic number	创建基本 ACL
acl advanced number	创建高级 ACL
description text	配置 ACL 的描述信息
rule { deny | permit } [fragment | logging| source ×.×.×.× ×.×.×.×| any |time-range name | vpn-instance name]	创建规则
packet-filter acl-number inbound	ACL 引入

实验 1　配置基本 ACL

实验目的:学会怎么配置基本 ACL,掌握如何更好地管理内部网络。

实验器材：H3C S5820 一台。

实验要求：

(1) 在每天的 8～18 点只允许 PC_1 和 PC_2 的报文通过。

(2) 用 ACL 2001 定义 PC_1 的报文通过。

(3) 用 ACL 2002 定义 PC_2 的报文通过。

基本 ACL 的配置拓扑图如图 7-1 所示。

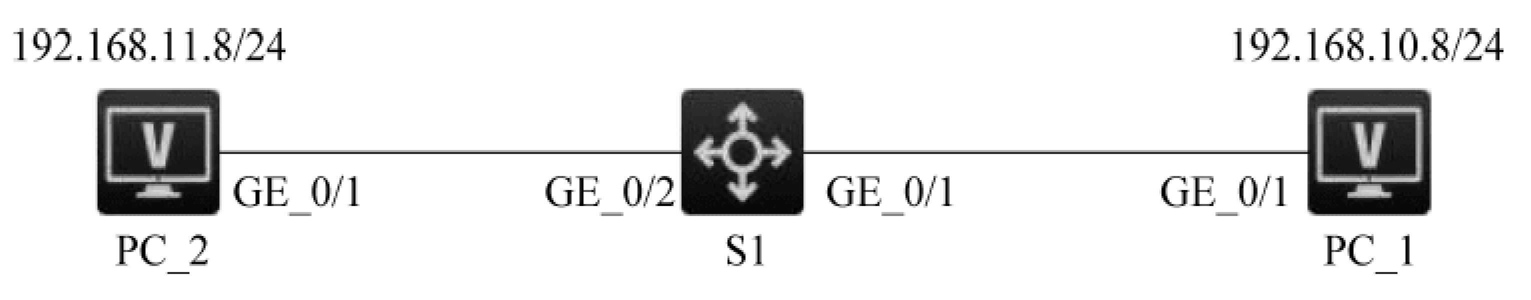


图 7-1　基本 ACL 的配置拓扑图

实验步骤如下：

```
[S1]time-range work 8:0 to 18:0 daily
  //创建时间范围为 8~18 点,名称为 work
[S1]acl basic 2001
[S1-acl-ipv4-basic-2001]rule permit source 192.168.10.8 0 time-range work logging
  //在名称为 work 的时间段内只允许来自 PC_1(192.168.10.8)的报文通过
[S1-acl-ipv4-basic-2001]rule deny source any time-range work logging
  //在名称为 work 的时间段内禁止来自其他 IP 地址的报文通过
[S1-acl-ipv4-basic-2001]quit
[S1]interface GigabitEthernet 1/0/1
[S1-GigabitEthernet1/0/1]packet-filter 2001 inbound
  //在端口上应用 ACL 2001
[S1-GigabitEthernet1/0/1]quit
[S1]acl basic 2002
[S1-acl-ipv4-basic-2002]rule permit source 192.168.11.8 0 time-range work logging
[S1-acl-ipv4-basic-2002]rule deny source any time-range work logging
[S1-acl-ipv4-basic-2002]quit
[S1]interface GigabitEthernet 1/0/2
[S1-GigabitEthernet1/0/2]packet-filter 2002 inbound
```

PC_1 的配置如图 7-2 所示。

PC_2 的配置如图 7-3 所示。

实验结果如下：

```
[S1]display acl all
Basic IPv4 ACL 2001, 2 rules, ACL's step is 5
rule 0 permit source 192.168.10.8 0 logging time-range work (Inactive)
rule 5 deny logging time-range work (Inactive) Basic IPv4 ACL 2002, 2 rules,
ACL's step is 5
rule 0 permit source 192.168.11.8 0 logging time-range work (Inactive)
rule 5 deny logging time-range work (Inactive)
```



图 7-2　PC_1 的配置



图 7-3　PC_2 的配置

实验 2　配置高级 ACL

实验目的：掌握高级 ACL 的配置方法。

实验器材：H3C MSR36-20 三台、PC 三台。

实验要求：

（1）为了合理利用带宽，规划从 R1 到 R2 的 FTP 数据通过 R1～R2 线路转发，从 R1～R3 的 Web 数据通过 R1～R3 的线路转发。

（2）R1～R2 的 FTP 数据由 ACL 3001 定义。

（3）R1～R3 的 Web 数据由 ACL 3002 定义。

高级 ACL 的配置拓扑图如图 7-4 所示。

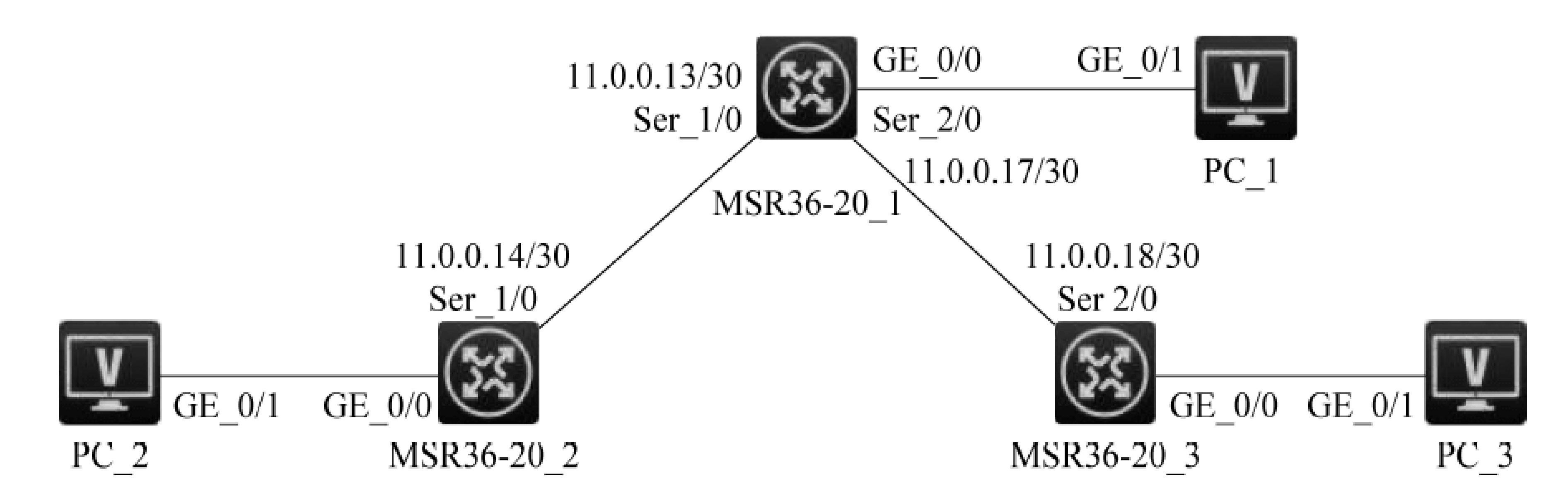


图 7-4　高级 ACL 的配置拓扑图

实验步骤如下：

```
[R1]interface Serial 1/0
[R1-Serial1/0]ip address 11.0.0.13 30
[R1]interface s
[R1]interface Serial 2/0
[R1-Serial2/0]ip address 11.0.0.17 30
[R1]acl advanced 3001
[R1-acl-ipv4-adv-3001]rule permit tcp destination-port eq ftp
[R1-acl-ipv4-adv-3001]rule permit tcp destination-port eq ftp-data
[R1]policy-based-route 1 permit node 2
[R1-pbr-1-2]apply next-hop 11.0.0.14
[R1]interface GigabitEthernet 0/0
[R1-GigabitEthernet0/0]ip policy-based-route 1
[R1]acl advanced 3002
[R1-acl-ipv4-adv-3002]rule permit tcp destination-port eq www
[R1]policy-based-route 1 permit node 3
[R1-pbr-1-3]apply next-hop 11.0.0.18
[R1]interface GigabitEthernet 0/0
[R1-GigabitEthernet0/0]ip policy-based-route 1

[R2]interface Serial 1/0
[R2-Serial1/0]ip address 11.0.0.14 30
```

```
[R2]acl advanced 3001
[R2-acl-ipv4-adv-3001]rule permit tcp destination-port eq ftp
[R2-acl-ipv4-adv-3001]rule permit tcp destination-port eq ftp-data
[R2]policy-based-route 1 permit node 2
[R2-pbr-1-2]apply next-hop 11.0.0.13
[R2]interface GigabitEthernet 0/0
[R2-GigabitEthernet0/0]ip policy-based-route 1

[R3]interface Serial 2/0
[R3-Serial2/0]ip address 11.0.0.18 30
[R3]acl advanced 3002
[R3-acl-ipv4-adv-3002]rule permit tcp destination-port eq www
[R3]policy-based-route 1 permit node 2
[R3-pbr-1-2]apply next-hop 11.0.0.17
[R3]interface GigabitEthernet 0/0
[R3-GigabitEthernet0/0]ip policy-based-route 1
```

实验结果如下：

```
[R1]display acl all
Advanced IPv4 ACL 3001, 2 rules, ACL's step is 5
rule 0 permit tcp destination-port eq ftp
rule 5 permit tcp destination-port eq ftp-data

Advanced IPv4 ACL 3002, 1 rule, ACL's step is 5
rule 0 permit tcp destination-port eq www

[R2]display acl all
Advanced IPv4 ACL 3001, 2 rules, ACL's step is 5
rule 0 permit tcp destination-port eq ftp
rule 5 permit tcp destination-port eq ftp-data

[R2]display acl all
Advanced IPv4 ACL 3001, 2 rules, ACL's step is 5
rule 0 permit tcp destination-port eq ftp
rule 5 permit tcp destination-port eq ftp-data
```

7.2 QoS 简介

QoS 即服务质量。对于网络业务，影响服务质量的因素包括传输的带宽、传送的时延、数据的丢包率等。在网络中可以通过保证传输的带宽、降低传送的时延、降低数据的丢包率以及时延抖动等措施来提高服务质量。在正常情况下，如果网络只用于特定的无时间限制的应用系统，则不需要 QoS，如 Web 应用或 E-mail 设置等。但是对关键应用和多媒体应用就十分必要。

7.2.1 QoS 服务模型简介

通常 QoS 提供以下三种服务模型：Best-Effort Service(尽力而为服务模型)、Integrated Service(综合服务模型，简称 IntServ)、Differentiated Service(区分服务模型，简称 DiffServ)。

Best-Effort 是一个单一的服务模型，也是最简单的服务模型。对 Best-Effort 服务模型，网络尽最大可能性来发送报文，但对时延、可靠性等性能不提供任何保证。Best-Effort 服务模型是网络的默认服务模型，通过 FIFO 队列来实现。它适用于绝大多数网络应用，如 FTP、E-mail 等。

IntServ 是一个综合服务模型，它可以满足多种 QoS 需求。该模型使用 RSVP，RSVP 运行在从源端到目的端的每台设备上，可以监视每个流，以防止其消耗资源过多。这种体系能够明确区分并保证每一个业务流的服务质量，为网络提供最细粒度化的服务质量区分。但是，IntServ 服务模型对设备的要求很高，当网络中的数据流数量很大时，设备的存储和处理能力会遇到很大的压力。IntServ 服务模型可扩展性很差，难以在 Internet 核心网络中实施。

DiffServ 是一个多服务模型，它可以满足不同的 QoS 需求。与 IntServ 不同，它不需要通知网络为每个业务预留资源。区分服务实现简单，扩展性较好。

7.2.2 QoS 的配置方式

QoS 配置方式分为非 QoS 策略配置方式和 QoS 策略配置方式。非 QoS 策略配置方式是指不通过 QoS 策略进行配置。例如，接口限速功能可以通过直接在接口上配置实现。QoS 策略配置方式是指通过配置 QoS 策略实现 QoS 功能。

QoS 策略包含三个要素：类、流行为和策略。用户可以通过 QoS 策略将指定的类和流行为绑定起来，灵活地进行 QoS 配置。

7.2.3 优先级映射介绍

优先级用于标识报文传输的优先程度，可以分为两类：报文携带优先级和设备调度优先级。报文携带优先级包括 802.1p 优先级、DSCP 优先级、IP 优先级、EXP 优先级等。这些优先级都是根据公认的标准和协议生成，体现了报文自身的优先等级。设备调度优先级是指报文在设备内转发时所使用的优先级，只对当前设备自身有效。设备调度优先级包括以下几种。

本地优先级(LP)：设备为报文分配的一种具有本地意义的优先级，每个本地优先级对应一个队列，本地优先级值越大的报文，进入的队列优先级越高，从而能够获得优先的调度。

用户优先级(UP)：设备对于进入的流量，会自动获取报文的优先级作为后续转发调

度的参数，这种报文优先级称为用户优先级。对于不同类型的报文，用户优先级所代表的优先级字段不同。对于二层报文，用户优先级取自 802.1p 优先级；对于三层报文，用户优先级取自 IP 优先级；对于 MPLS 报文，用户优先级取自 EXP 优先级。

7.2.4 QoS 的配置命令

表 7-2 所示是配置 QoS 时所需用到的一些命令。

表 7-2　QoS 的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
traffic classifier name	设置 Classifier 名称
traffic behavior name	设置 Behavior 名称
qos policy name name	设置 QoS 名称
qos apply policy name outbound	引入 QoS 策略
classifier name behavior name	将 Classifier 和 Behavior 引入 QoS 策略中

实验 3　配置 QoS 部署

实验目的：知道如何配置 QoS，并掌握相关的命令。

实验器材：H3C MSR36-20 三台、PC 一台。

实验背景：某公司将 R1 所在区域列为分部，将 R2、R3 所在区域列为总部，为保证能应用广域网带宽，需要在设备上配置 QoS。

实验要求：要使分部与总部 DNS 服务器(192.168.10.100/24)间的 DNS 数据流能够被加速转发(EF)，最大带宽为链路带宽的 20%；ACL 编号为 3003(匹配 DNS 数据流)；Classifier 名称为 DNS；Behavior 名称为 DNS；QoS 策略名称为 DNS。

QoS 部署的配置拓扑图如图 7-5 所示。

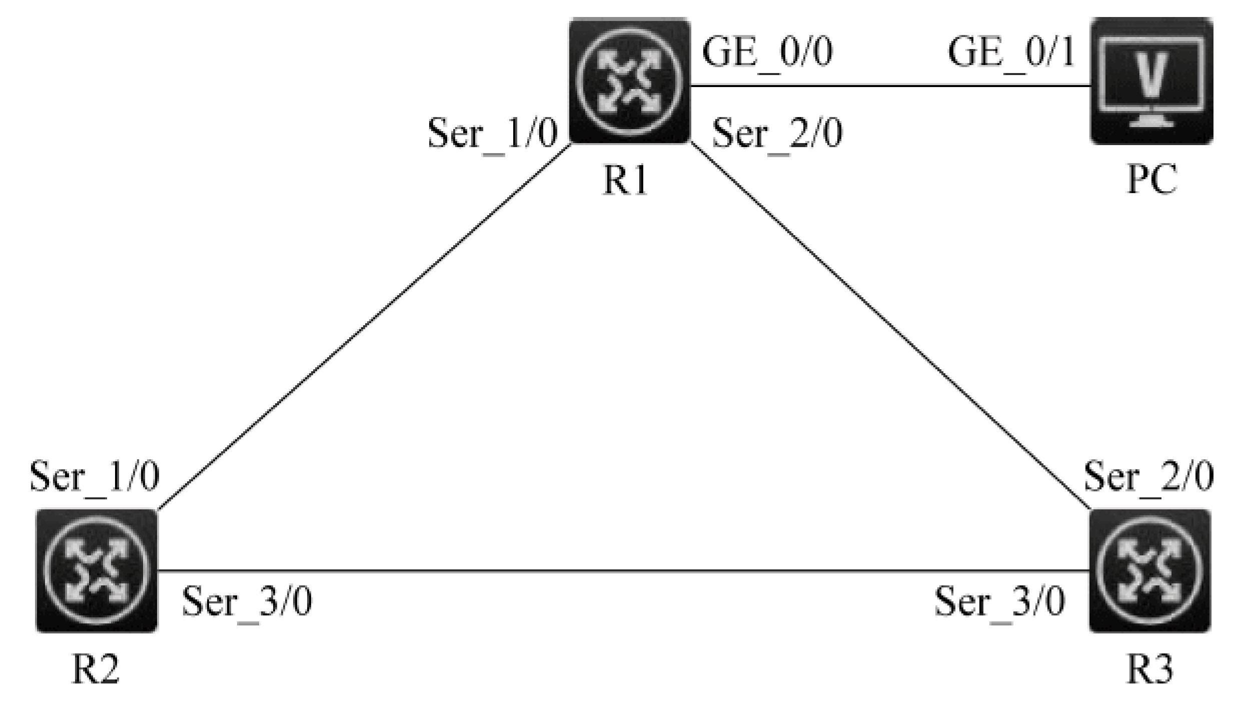


图 7-5　QoS 部署的配置拓扑图

实验步骤如下：

```
[R1]acl advanced 3003
[R1-acl-ipv4-adv-3003]rule permit ip destination 192.168.10.100 0
[R1-acl-ipv4-adv-3003]quit
[R1]traffic classifier DNS
[R1-classifier-DNS]if-match acl 3003
[R1-classifier-DNS]quit
[R1]traffic behavior DNS
[R1-behavior-DNS]queue ef bandwidth pct 20
[R1-behavior-DNS]quit
[R1]qos policy DNS
[R1-qospolicy-DNS]classifier DNS behavior DNS
[R1-qospolicy-DNS]quit
[R1]interface Serial 2/0
[R1-Serial2/0]qos apply policy DNS outbound
[R1]interface Serial 1/0
[R1-Serial1/0]qos apply policy DNS outbound

[R2]acl advanced 3003
[R2-acl-ipv4-adv-3003]rule permit ip destination 192.168.10.100 255.255.255.0
[R2-acl-ipv4-adv-3003]quit
[R2]traffic classifier DNS
[R2-classifier-DNS]if-match acl 3003
[R2-classifier-DNS]quit
[R2]traffic behavior DNS

[R2-behavior-DNS]queue ef bandwidth pct 20
[R2-behavior-DNS]quit
[R2]qos policy DNS
[R2-qospolicy-DNS]classifier DNS behavior DNS
[R2-qospolicy-DNS]quit
[R2]interface Serial 1/0
[R2-Serial1/0]qos apply policy DNS outbound
[R3]acl advanced 3003
[R3-acl-ipv4-adv-3003]rule permit ip destination 192.168.10.100 255.255.255.0
[R3-acl-ipv4-adv-3003]quit
[R3]traffic classifier DNS
[R3-classifier-DNS]if-match acl 3003
[R3-classifier-DNS]quit
[R3]traffic behavior DNS
[R3-behavior-DNS]queue ef bandwidth pct 20
[R3-behavior-DNS]quit
[R3]qos policy DNS
[R3-qospolicy-DNS]classifier DNS behavior DNS
[R3-qospolicy-DNS]quit
[R3]interface Serial 2/0
[R3-Serial2/0]qos apply policy DNS outbound
```

PC 的配置如图 7-6 所示。



图 7-6 PC 的配置

实验结果如下：

```
[R1]display qos policy interface
Interface: Serial1/0
Direction: Outbound
Policy: DNS
    Classifier: default-class
    Matched: 0 (Packets) 0 (Bytes)
    5-minute statistics:
    Forwarded: 0/0 (pps/bps)
    Dropped: 0/0 (pps/bps)
    Operator: AND
    Rule(s):
    If-match any
    Behavior: be
    Default Queue:
    Flow based Weighted Fair Queue:

Max number of hashed queues: 256
    Matched: 0 (Packets) 0 (Bytes)
    Enqueued: 0 (Packets) 0 (Bytes)
    Discarded: 0 (Packets) 0 (Bytes)
    Discard Method: Tail
```

```
Classifier: DNS
    Matched: 0 (Packets) 0 (Bytes)
    5-minute statistics: Forwarded:
    0/0 (pps/bps) Dropped: 0/0
    (pps/bps) Operator: AND
    Rule(s):
If-match acl 3003
Behavior: DNS
    Expedited Forwarding:
    Bandwidth 10 (kbps) CBS 250 (Bytes)
    Matched: 0 (Packets) 0 (Bytes)
    Enqueued: 0 (Packets) 0 (Bytes)
    Discarded: 0 (Packets) 0 (Bytes) Discard
    Method: Tail

Interface: Serial2/0
  Direction: Outbound
Policy: DNS
    Classifier: default-class
    Matched: 0 (Packets) 0 (Bytes)
    5-minute statistics:
    Forwarded: 0/0 (pps/bps)
    Dropped : 0/0 (pps/bps)
    Operator: AND
    Rule(s):
    If-match any
    Behavior: be
    Default Queue:
    Flow based Weighted Fair Queue:
    Max number of hashed queues: 256
    Matched: 0 (Packets) 0 (Bytes)
    Enqueued: 0 (Packets) 0 (Bytes)
    Discarded: 0 (Packets) 0 (Bytes)
    Discard Method: Tail
Classifier: DNS
    Matched: 0 (Packets) 0 (Bytes)
    5-minute statistics:
    Forwarded: 0/0 (pps/bps)
    Dropped : 0/0 (pps/bps)
    Operator: AND
    Rule(s):
If-match acl 3003
Behavior: DNS
    Expedited Forwarding:
    Bandwidth 10 (kbps) CBS 250 (Bytes)
    Matched: 0 (Packets) 0 (Bytes)
    Enqueued: 0 (Packets) 0 (Bytes)
    Discarded: 0 (Packets) 0 (Bytes) Discard
    Method: Tail
```

```
[R2]display qos policy interface
Interface: Serial1/0
    Direction: Outbound
Policy: DNS
    Classifier: default-class
    Matched: 0 (Packets) 0 (Bytes)
    5-minute statistics:
    Forwarded: 0/0 (pps/bps)
    Dropped : 0/0 (pps/bps)
    Operator: AND
    Rule(s):
    If-match any
    Behavior: be
    Default Queue:
    Flow based Weighted Fair Queue:
Max number of hashed queues: 256
    Matched: 0 (Packets) 0 (Bytes)
    Enqueued: 0 (Packets) 0 (Bytes)
    Discarded: 0 (Packets) 0 (Bytes)
    Discard Method: Tail
Classifier: DNS
    Matched: 0 (Packets) 0 (Bytes)
    5-minute statistics:
    Forwarded: 0/0 (pps/bps)
    Dropped: 0/0 (pps/bps)
    Operator: AND
    Rule(s):
If-match acl 3003
Behavior: DNS
    Expedited Forwarding:
    Bandwidth 10 (kbps) CBS 250 (Bytes)
    Matched: 0 (Packets) 0 (Bytes)
    Enqueued: 0 (Packets) 0 (Bytes)
    Discarded: 0 (Packets) 0 (Bytes)
    Discard Method: Tail

[R3]display qos policy interface
Interface: Serial2/0
  Direction: Outbound
Policy: DNS
    Classifier: default-class
    Matched: 0 (Packets) 0 (Bytes)
    5-minute statistics:
    Forwarded: 0/0 (pps/bps)
    Dropped : 0/0 (pps/bps)
    Operator: AND
    Rule(s):
    If-match any
    Behavior: be
```

```
    Default Queue:
    Flow based Weighted Fair Queue:
Max number of hashed queues: 256
    Matched: 0 (Packets) 0 (Bytes)
    Enqueued: 0 (Packets) 0 (Bytes)
    Discarded: 0 (Packets) 0 (Bytes)
    Discard Method: Tail
Classifier: DNS
    Matched: 0 (Packets) 0 (Bytes)
    5-minute statistics:
    Forwarded: 0/0 (pps/bps)
    Dropped : 0/0 (pps/bps)
    Operator: AND
    Rule(s):
If-match acl 3003
Behavior: DNS
    Expedited Forwarding:
    Bandwidth 10 (kbps) CBS 250 (Bytes)
    Matched: 0 (Packets) 0 (Bytes)
    Enqueued: 0 (Packets) 0 (Bytes)
    Discarded: 0 (Packets) 0 (Bytes) Discard
    Method: Tail
```

项目 8 IPSec 配置

8.1 IPSec 简介

IPSec(IP Security,IP 安全)是 IETF 制定的三层隧道加密协议,它为互联网上传输的数据提供了高质量的、基于密码学的安全保证,是一种传统的实现三层 VPN(Virtual Private Network,虚拟专用网络)的安全技术。IPSec 通过在特定通信方之间(如两个安全网关之间)建立“通道”,来保护通信方之间传输的用户数据,该通道通常称为 IPSec 隧道。

8.1.1 IPSec 的安全服务

IPSec 为 IP 层的数据报文提供的安全服务具体包括以下几种。

数据机密性(Confidentiality):发送方通过网络传输用户报文前,IPSec 对报文进行加密。

数据完整性(Data Integrity):接收方对发送方发送来的 IPSec 报文进行认证,以确保数据在传输过程中没有被篡改。

数据来源认证(Data Authentication):接收方认证发送 IPSec 报文的发送端是否合法。

抗重放(Anti-Replay):接收方可检测并拒绝接收过时或重复的 IPSec 报文。

8.1.2 IPSec 的认证和加密

1. 认证算法

IPSec 使用的认证算法主要是通过杂凑函数实现的。杂凑函数是一种能够接收任意长度的消息输入,并产生固定长度输出的算法,该算法的输出称为消息摘要。IPSec 对等体双方都会计算一个摘要,接收方将发送方的摘要与本地的摘要进行比较,如果二者相同,则表示收到的 IPSec 报文是完整未被篡改的,以及发送方身份合法。目前,IPSec 强制使用基于 HMAC(Hash-based Message Authentication Code,基于散列的消息鉴别码)的认证算法,包括 HMAC-MD5 和 HMAC-SHA1。其中,HMAC-MD5 算法的计算速度快,而 HMAC-SHA1 算法的安全强度高。

2. 加密算法

IPSec 使用的加密算法属于对称密钥系统，这类算法使用相同的密钥对数据进行加密和解密。目前设备的 IPSec 使用三种加密算法。

DES：使用 56bit 的密钥对一个 64bit 的明文块进行加密。

3DES：使用三个 56bit(共 168bit)的密钥对明文块进行加密。

AES：使用 128bit、192bit 或 256bit 的密钥对明文块进行加密。这三个加密算法的安全性由高到低依次是 AES、3DES、DES，安全性高的加密算法实现机制复杂，运算速度慢。

8.1.3 IPSec 的优点

IPSec 支持 IKE(Internet Key Exchange，互联网密钥交换)，可实现密钥的自动协商功能，减少了密钥协商的开销。可以通过 IKE 建立和维护 SA(Security Association，安全联盟)，简化了 IPSec 的使用和管理。

所有使用 IP 协议进行数据传输的应用系统和服务都可以使用 IPSec，而不必对这些应用系统和服务本身做任何修改。

对数据的加密是以数据包为单位的，而不是以整个数据流为单位，这不但灵活，而且有助于进一步提高 IP 数据包的安全性，可以有效防范网络攻击。

8.2 IKE 简 介

IKE 协议利用 ISAKMP(Internet Security Association and Key Management Protocol，互联网安全联盟和密钥管理协议)语言定义密钥交换的过程，是一种对安全服务进行协商的手段。

用 IPSec 保护一个 IP 数据包之前，必须先建立一个安全联盟(IPSec SA)，IPSec SA 可以手动或动态建立。IKE 可用于协商虚拟专用网(VPN)，也可用于远程用户(其 IP 地址不需要事先知道)访问安全主机或网络，支持客户端协商。客户端模式即为协商方不是安全连接发起的终端点。当使用客户端模式时，端点处身份是隐藏的。

8.2.1 IKE 的安全机制

IKE 可以在不安全的网络上安全地认证通信双方的身份、分发密钥以及建立 IPSec SA，具有以下三种安全机制。

1. 身份认证

IKE 的身份认证机制用于确认通信双方的身份。设备支持三种认证方法：预共享密

钥认证、RSA 数字签名认证和 DSA 数字签名认证。

预共享密钥认证：通信双方通过共享的密钥认证对端身份。

RSA 或 DAS 数字签名认证：通信双方使用由 CA 颁发的数字证书向对端证明自己的身份。

2. DH 算法

DH 算法是一种公共密钥算法，它允许通信双方在不传输密钥的情况下通过交换一些数据，计算出共享的密钥。即使第三方(如黑客)截获了双方用于计算密钥的所有交换数据，由于其复杂度很高，也不足以计算出双方的密钥。

3. PFS 特性

PFS(Perfect Forward Secrecy，完善的前向安全性)是一种安全特性，它解决了密钥之间相互无关性的需求。由于 IKE 第二阶段协商需要从第一阶段协商出的密钥材料中衍生出用于 IPSec SA 的密钥，若攻击者能够破解 IKE SA 的一个密钥，则会非常容易地掌握其衍生出的任何 IPSec SA 的密钥。使用 PFS 特性后，IKE 第二阶段协商过程中会增加一次 DH 交换，使得 IKE SA 的密钥和 IPSec SA 的密钥之间没有派生关系，即使 IKE SA 的其中一个密钥被破解，也不会影响它协商出的其他密钥的安全性。

8.2.2 IKE 的优点

IKE 首先会在通信双方之间协商建立一个安全通道(IKE SA)，并在此安全通道的保护下协商建立 IPSec SA，这降低了手动配置的复杂度，简化了 IPSec 的配置和维护工作。IKE 的精髓在于 DH(Diffie-Hellman)交换技术，它通过一系列的交换，使得通信双方最终计算出共享密钥。在 IKE 的 DH 交换过程中，每次计算和产生的结果都是不相关的。由于每次 IKE SA 的建立都运行了 DH 交换过程，因此就保证了每个通过 IKE 协商建立的 IPSec SA 所使用的密钥互不相关。

IPSec 使用 AH 或 ESP 报文头中的顺序号实现防重放。此顺序号是一个 32 比特的值，此数溢出之前，为实现防重放，IPSec SA 需要重新建立，IKE 可以自动重协商 IPSec SA。

8.2.3 IPSec 的配置命令

表 8-1 所示是配置 IPses 时所需用到的一些命令。

表 8-1　IPSec 的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
ipsec transform-set name	创建 IPSec 安全协议

续表

操 作 命 令	操 作 说 明
encapsulation-mode {transport|tunnel}	配置安全协议对 IP 报文的封装形式
protocol {ah|ah-esp|esp}	配置采用的安全协议
ipsec policy name number manual	创建一条手动方式的 IPSec 安全策略
ipsec apply policy name	应用 IPSec 安全策略
ike keychain name	创建一个 IKE 密钥的名称

实验 1　采用手动方式建立保护 IPv4 报文的 IPSec 隧道

实验目的：掌握手动配置 IPSec 的方式。

实验器材：H3C MSR36-20 两台、PC 两台。

实验要求：

(1) 在 Router A 和 Router B 之间建立一条 IPSec 隧道，对 Host A 所在的子网(10.1.1.0/24)与 Host B 所在的子网(10.1.2.0/24)之间的数据流进行安全保护。

(2) 封装形式为隧道模式。

(3) 安全协议采用 ESP 协议。

(4) 加密算法采用 128 比特的 AES，认证算法采用 HMAC-SHA1 手动方式建立 IPSec SA。

IPSec 的手动配置方式拓扑图如图 8-1 所示。

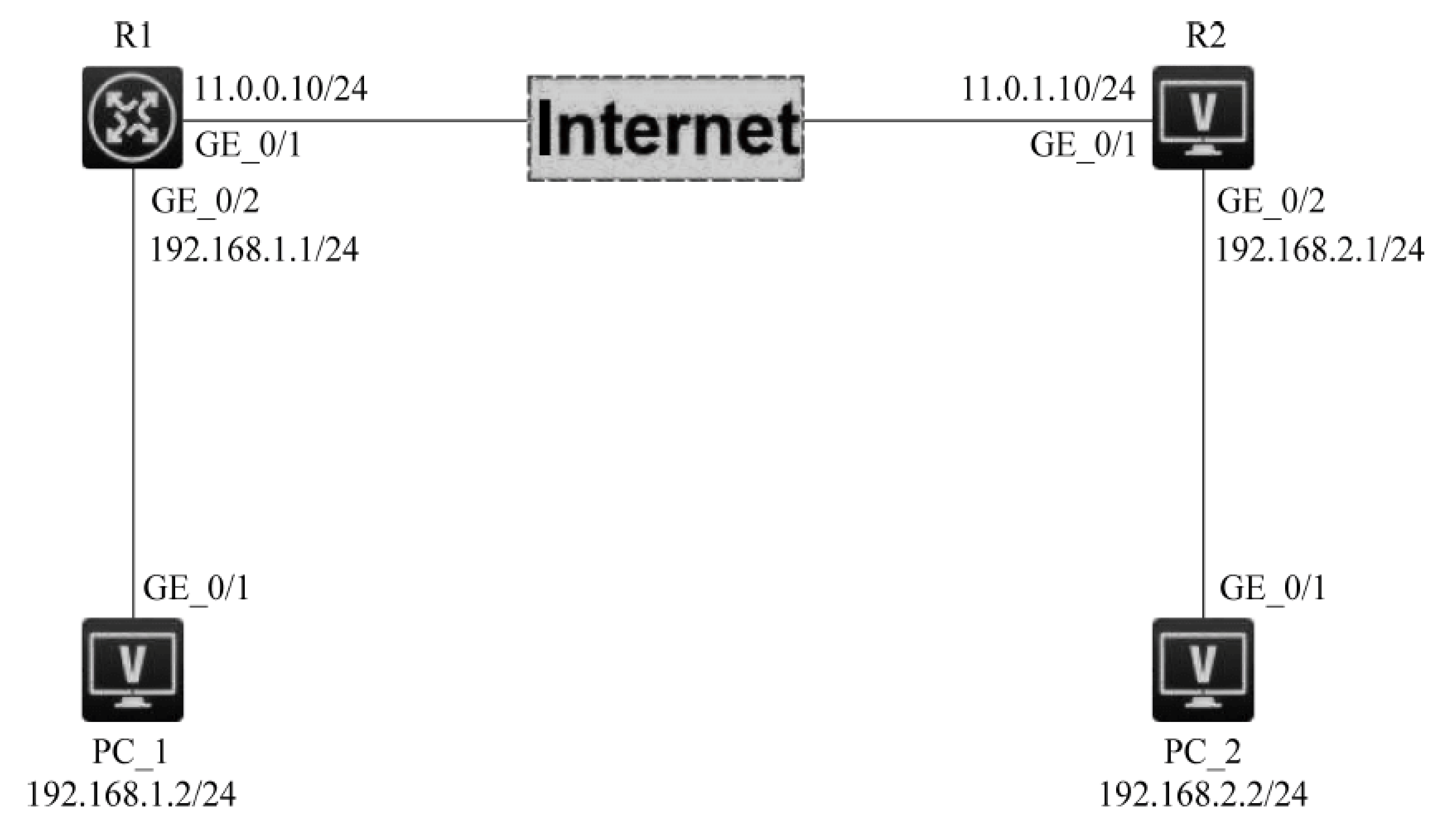


图 8-1　IPSec 的手动配置方式拓扑图

实验步骤如下：

```
[R1]interface GigabitEthernet 0/1
```

```
[R1-GigabitEthernet0/1]ip address 11.0.0.10 24
[R1-GigabitEthernet0/1]quit
[R1]interface GigabitEthernet 0/2
[R1-GigabitEthernet0/2]ip address 192.168.1.1 24
[R1] acl number 3101
  //配置一个 ACL,定义要保护的由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流
[R1-acl-adv-3101] rule permit ip source 192.168.1.2.0.0.255 destination
192.168.2.2 0.0.0.255
[R1] ip route-static 192.168.2.2255.255.255.0 gigabitethernet 0/1 11.0.0.9
  //配置到达 R2 所在子网的静态路由。11.0.0.9 为本例中直连的下一跳地址,实际使用中请以具
    体组网情况为准
[R1] ipsec transform-set tran1                      //创建 IPSec 安全提议 tran1
[R1-ipsec-transform-set-tran1] encapsulation-mode tunnel
  //配置安全协议时对 IP 报文的封装形式为隧道模式
[R1-ipsec-transform-set-tran1] protocol esp          //配置采用的安全协议为 ESP
[R-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
  //配置 ESP 协议采用的加密算法为采用 128 比特的 AES
[R1-ipsec-transform-set-tran1] esp authentication-algorithm sha1
  //认证算法为 HMAC-SHA1
[R1-ipsec-transform-set-tran1] quit
[R1] ipsec policy map1 10 manual
  //创建一条手动方式的 IPSec 安全策略,名称为 map1,序列号为 10
[R1-ipsec-policy-manual-map1-10] security acl 3101
  //指定引用 ACL 3101
[R1-ipsec-policy-manual-map1-10] transform-set tran1
  //指定引用的 IPSec 安全提议为 tran1
[R1-ipsec-policy-manual-map1-10] remote-address 11.0.1.10
  //指定 IPSec 隧道的端 IP 地址为 11.0.1.10
[R1-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
  //配置 ESP 协议的出口方向 SPI 为 12345
[R1-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
  //入口方向 SPI 为 54321
[R1-ipsec-policy-manual-map1-10] sa string-key outbound esp simple abcdefg
  //配置 ESP 协议的出口方向 SA 的密钥为明文字符串 abcdefg
[R1-ipsec-policy-manual-map1-10] sa string-key inbound esp simple gfedcba
  //入口方向 SA 的密钥为明文字符串 gfedcba
[R1-ipsec-policy-manual-map1-10] quit
[R1] interface gigabitethernet 0/1
[R1-GigabitEthernet0/1] ip address 11.0.0.10 255.255.255.0
[R1-GigabitEthernet0/1] ipsec apply policy map1
  //在接口 GigabitEthernet0/1 上应用 IPSec 安全策略 map1
[R1-GigabitEthernet0/1] quit

[R2]interface GigabitEthernet 0/1
[R2-GigabitEthernet0/1]IP address 11.0.1.10 24
[R2-GigabitEthernet0/1]interface GigabitEthernet 0/2
[R2-GigabitEthernet0/2]IP address 192.168.2.1 24
[R2] acl number 3101
[R2-acl-adv-3101] rule permit ip source 192.168.2.2 0.0.0.255 destination
```

```
192.168.1.2 0.0.0.255
[R2] ip route-static 192.168.1.2 255.255.255.0 gigabitethernet 0/1 11.0.1.9
  //配置到达 R1 所在子网的静态路由。11.0.1.9 为本例中直连的下一跳地址,实际使用中请以具
    体组网情况为准
[R2] ipsec transform-set tran1
[R2-ipsec-transform-set-tran1] encapsulation-mode tunnel
[R2-ipsec-transform-set-tran1] protocol esp
[R2-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[R2-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[R2] ipsec policy use1 10 manual
[R2-ipsec-policy-manual-use1-10] security acl 3101
[R2-ipsec-policy-manual-use1-10] transform-set tran1
[R2-ipsec-policy-manual-use1-10] remote-address 11.0.0.10
[R2-ipsec-policy-manual-use1-10] sa spi outbound esp 54321
[R2-ipsec-policy-manual-use1-10] sa spi inbound esp 12345
[R2-ipsec-policy-manual-use1-10] sa string-key outbound esp simple gfedcba
[R2-ipsec-policy-manual-use1-10] sa string-key inbound esp simple abcdefg
[R2-ipsec-policy-manual-use1-10] quit
[R2] interface gigabitethernet 0/1
[R2-GigabitEthernet0/1] ipsec apply policy use1
[R2-GigabitEthernet0/1] quit
```

PC_1 的配置如图 8-2 所示。



图 8-2　PC_1 的配置

PC_2 的配置如图 8-3 所示。

图 8-3　PC_2 的配置

实验结果如下：

```
[R1] display ipsec sa
--------------------------------Interface:
GigabitEthernet0/1
--------------------------------IPSec
    policy: map1
    Sequence number: 10
    Mode: manual
    ------------------------------Tunnel id:
        549
        Encapsulation mode: tunnel
        Path MTU: 1443
        Tunnel:
            local address: 11.0.0.10
            remote address: 11.0.1.10
        Flow:
            as defined in ACL 3101
        [Inbound ESP SA]
            SPI: 54321 (0x0000d431)
            Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
            No duration limit for this SA
```

```
        [Outbound ESP SA]
            SPI: 12345 (0x00003039)
            Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
            No duration limit for this SA

[R2] display ipsec sa
-------------------------------Interface:
GigabitEthernet0/1
-------------------------------IPSec
    policy: map1
    Sequence number: 10
    Mode: manual
    -----------------------------Tunnel id:
        549
        Encapsulation mode: tunnel
        Path MTU: 1443
        Tunnel:
            local address: 11.0.1.10
            remote address: 11.0.0.10
        Flow:
            as defined in ACL 3101
        [Inbound ESP SA]
            SPI: 54321 (0x0000d431)
            Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
            No duration limit for this SA
        [Outbound ESP SA]
            SPI: 12345 (0x00003039)
            Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
            No duration limit for this SA
```

实验 2　采用 IKE 方式建立保护 IPv4 报文的 IPSec 隧道

实验目的：掌握手动配置 IPSec 的方式。

实验器材：H3C MSR36-20 两台、PC 一台。

实验要求：

(1) 在 Router A 和 Router B 之间建立一条 IPSec 隧道，对 Host A 所在的子网(10.1.1.0/24)与 Host B 所在的子网(10.1.2.0/24)之间的数据流进行安全保护。

(2) 封装形式为隧道模式。

(3) 安全协议采用 ESP 协议。

(4) 加密算法采用 128 比特的 AES，认证算法采用 HMAC-SHA1。

(5) 以 IKE 协商方式建立 IPSec SA。

以 IKE 协商方式建立的 IPSec SA 配置拓扑图如图 8-4 所示。

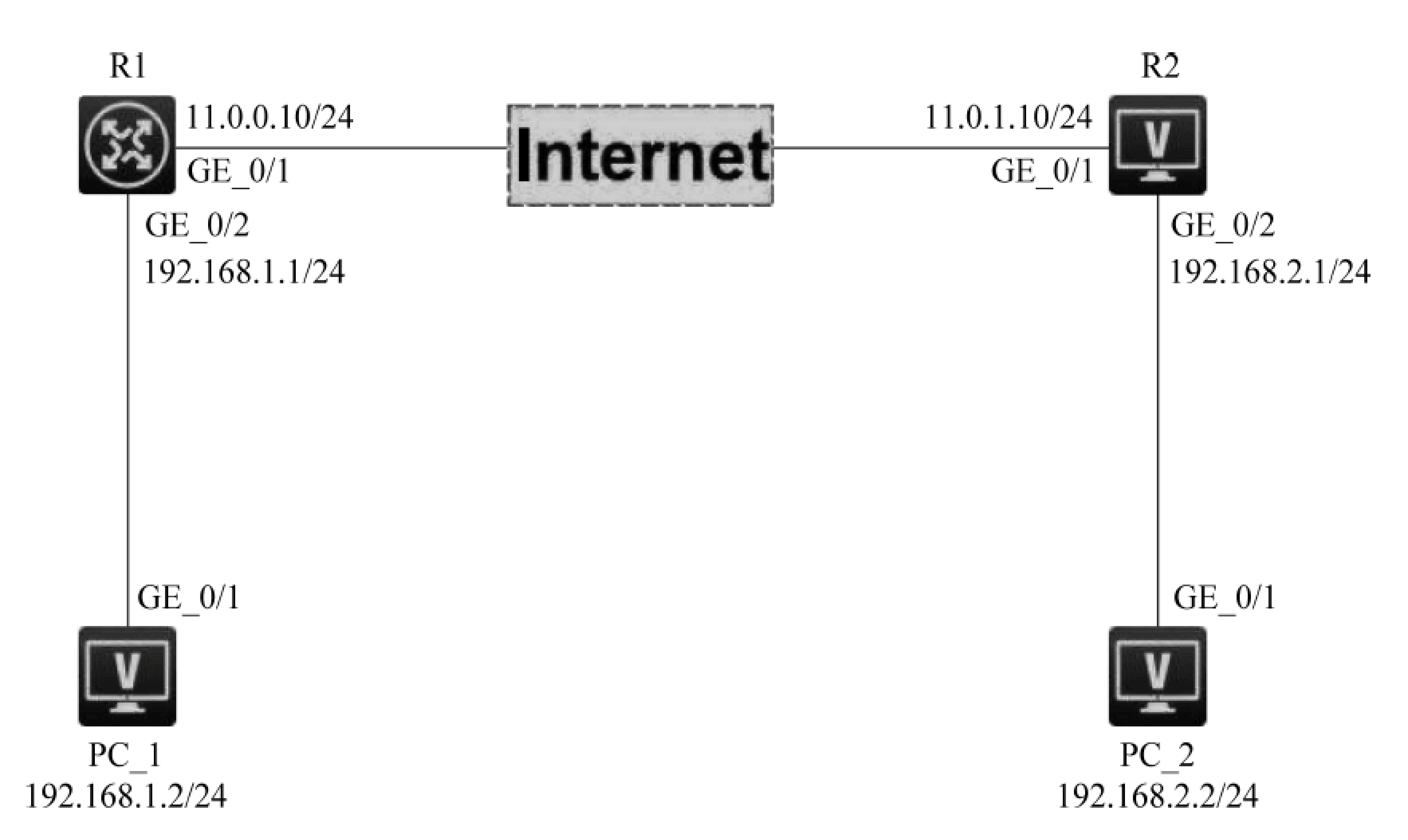


图 8-4　以 IKE 协商方式建立的 IPSec SA 配置拓扑图

实验步骤如下：

```
[R1]interface GigabitEthernet 0/1
[R1-GigabitEthernet0/1]ip address 11.0.0.10 24
[R1-GigabitEthernet0/1]quit
[R1]interface GigabitEthernet 0/2
[R1-GigabitEthernet0/2]ip address 192.168.1.1 24
[R1] acl number 3101
  //配置一个 ACL,定义要保护的由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流
[R1-acl-adv-3101] rule permit ip source 192.168.1.2.0.0.255 destination
192.168.2.2 0.0.0.255
[R1] ip route-static 192.168.2.2255.255.255.0 gigabitethernet 0/1 11.0.0.9
  //配置到达 R2 所在子网的静态路由。11.0.0.9 为本例中直连的下一跳地址,实际使用中请以具
    体组网情况为准
[R1] ipsec transform-set tran1                    //创建 IPSec 安全提议 tran1
[R1-ipsec-transform-set-tran1] encapsulation-mode tunnel
  //配置安全协议时对 IP 报文的封装形式为隧道模式
[R1-ipsec-transform-set-tran1] protocol esp       //配置采用的安全协议为 ESP
[R1-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
  //配置 ESP 协议采用的加密算法为采用 128 比特的 AES
[R1-ipsec-transform-set-tran1] esp authentication-algorithm sha1
  //认证算法为 HMAC-SHA1
[R1-ipsec-transform-set-tran1] quit
[R1] ike keychain keychain1
  //创建并配置 IKE keychain,名称为 keychain1
[R1-ike-keychain-keychain1] pre-shared-key address 11.0.1.10 255.255.255.0 key
simple 123456
  //配置与 IP 地址为 11.0.1.10 的对端使用的预共享密钥为明文 123456
[R1-ike-keychain-keychain1] quit
[R1] ike profile profile1
  //创建并配置 IKE profile,名称为 profile1
[R1-ike-profile-profile1] keychain keychain1
```

```
[R1-ike-profile-profile1] match remote identity address 11.0.1.10 255.255.255.0
[R1-ike-profile-profile1] quit
[R1] ipsec policy map1 10 isakmp
  //创建一条 IKE 协商方式的 IPSec 安全策略,名称为 map1,序列号为 10
[R1-ipsec-policy-isakmp-map1-10] security acl 3101
  //指定引用 ACL 3101
[R1-ipsec-policy-isakmp-map1-10] transform-set tran1
  //指定引用的安全提议为 tran1
[R1-ipsec-policy-isakmp-map1-10] local-address 11.0.0.10
  //指定 IPSec 隧道的本端 IP 地址为 11.0.0.10
[R1-ipsec-policy-isakmp-map1-10] remote-address 11.0.1.10
  //指定对端 IP 地址为 11.0.1.10
[R1-ipsec-policy-isakmp-map1-10] ike-profile profile1
  //指定引用的 IKE profile 为 profile1
[R1] interface gigabitethernet 0/1
[R1-GigabitEthernet0/1] ip address 2.2.2.1 255.255.255.0
[R1-GigabitEthernet0/1] ipsec apply policy map1
  //在接口 GigabitEthernet0/1 上应用安全策略 map1
[R1-GigabitEthernet0/1] quit

[R2]interface GigabitEthernet 0/1
[R2-GigabitEthernet0/1]IP address 11.0.1.10 24
[R2-GigabitEthernet0/1]interface GigabitEthernet 0/2
[R2-GigabitEthernet0/2]IP address 192.168.2.1 24
[R2] acl number 3101
[R2-acl-adv-3101] rule permit ip source 192.168.2.2 0.0.0.255 destination
192.168.1.2 0.0.0.255
[R2] ip route-static 192.168.1.2 255.255.255.0 gigabitethernet 0/1 11.0.1.9
  //配置到达 R1 所在子网的静态路由。11.0.1.9 为本例中直连的下一跳地址,实际使用中请以具
    体组网情况为准
[R2] ipsec transform-set tran1
[R2-ipsec-transform-set-tran1] encapsulation-mode tunnel
[R2-ipsec-transform-set-tran1] protocol esp
[R2-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[R2-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[R2] ike keychain keychain1
[R2-ike-keychain-keychain1] pre-shared-key address 11.0.0.10 255.255.255.0 key
simple 123456
[R2-ike-keychain-keychain1] quit
[R2] ike profile profile1
[R2-ike-profile-profile1] keychain keychain1
[R2-ike-profile-profile1] match remote identity address 11.0.0.10 255.255.255.0
[R2-ike-profile-profile1] quit
[R2] ipsec policy map1 10 isakmp
[R2-ipsec-policy-isakmp-map1-10] security acl 3101
[R2-ipsec-policy-isakmp-map1-10] transform-set tran1
[R2-ipsec-policy-isakmp-map1-10] local-address 11.0.1.10
[R2-ipsec-policy-isakmp-map1-10] remote-address 11.0.0.10
[R2-ipsec-policy-isakmp-map1-10] ike-profile profile1
```

```
[R2] interface gigabitethernet 0/1
[R2-GigabitEthernet0/1] ip address 11.0.1.10 255.255.255.0
[R2-GigabitEthernet0/1] ipsec apply policy map1
[R2-GigabitEthernet0/1] quit
```

PC_1 的配置如图 8-5 所示。



图 8-5 PC_1 的配置

PC_2 的配置如图 8-6 所示。

实验结果如下：

```
[R1] display ipsec sa
    -------------------------------Interface:
    GigabitEthernet0/1
    -------------------------------

    -----------------------------IPSec
    policy: map1
    Sequence number: 10
    Mode: isakmp
    -----------------------------Tunnel id:
        0
        Encapsulation mode: tunnel
        Perfect Forward Secrecy: Path
        MTU: 1443
```



图 8-6 PC_2 的配置

```
Tunnel:
    local address: 11.0.0.10
    remote address: 11.0.1.10
Flow:
    sour addr: 11.0.0.10/0.0.0.0    port: 0    protocol: IP
    dest addr: 11.0.1.10/0.0.0.0    port: 0    protocol: IP

[Inbound ESP SAs]
    SPI: 3769702703 (0xe0b1192f)
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 3000/28800
    SA remaining duration (kilobytes/sec): 2300/797
    Max received sequence-number: 1
    Anti-replay check enable: N
    Anti-replay window size:
    UDP encapsulation used for NAT traversal: N
    Status: active

[Outbound ESP SAs]
    SPI: 3840956402 (0xe4f057f2)
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 3000/28800
    SA remaining duration (kilobytes/sec): 2312/797
```

```
            Max sent sequence-number: 1
            UDP encapsulation used for NAT traversal: N
            Status: active

[R2] display ipsec sa
    -------------------------------Interface:
    GigabitEthernet0/1
    -------------------------------

    -----------------------------IPSec
    policy: map1
    Sequence number: 10
    Mode: isakmp
    -----------------------------Tunnel id:
        0
        Encapsulation mode: tunnel
        Perfect Forward Secrecy: Path
        MTU: 1443
    Tunnel:
        local address: 11.0.1.10
        remote address: 11.0.0.10
    Flow:
        sour addr: 11.0.1.10/0.0.0.0    port: 0    protocol: IP
        dest addr: 11.0.0.10/0.0.0.0    port: 0    protocol: IP

    [Inbound ESP SAs]
        SPI: 3769702703 (0xe0b1192f)
        Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
        SA duration (kilobytes/sec): 3000/28800
        SA remaining duration (kilobytes/sec): 2300/797
        Max received sequence-number: 1
        Anti-replay check enable: N Anti-
        replay window size:
        UDP encapsulation used for NAT traversal: N
        Status: active

    [Outbound ESP SAs]
        SPI: 3840956402 (0xe4f057f2)
        Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
        SA duration (kilobytes/sec): 3000/28800
        SA remaining duration (kilobytes/sec): 2312/797
        Max sent sequence-number: 1
        UDP encapsulation used for NAT traversal: N
        Status: active
```

项目 9　网络管理

9.1　SSH 简介

SSH 是 Secure Shell(安全外壳)的简称,是一种在不安全的网络环境中,通过加密机制和认证机制,实现安全的远程访问以及文件传输等业务的网络安全协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。

9.1.1　SSH 的认证方式

(1) password 认证:利用 AAA(Authentication、Authorization、Accounting,认证、授权和记账)对客户端身份进行认证。客户端向服务器发出 password 认证请求,将用户名和密码加密后发送给服务器;服务器将认证请求解密后得到用户名和密码的明文,通过本地认证或远程认证验证用户名和密码的合法性,并返回认证成功或失败的消息。

(2) publickey 认证:采用数字签名的方式认证客户端。目前,设备上可以利用 DSA 和 RSA 两种公钥算法实现数字签名。客户端发送包含用户名、公钥和公钥算法或者携带公钥信息的数字证书的 publickey 认证请求给服务器端。服务器端对公钥进行合法性检查,如果不合法,则直接发送失败消息;否则,服务器端利用数字签名对客户端进行认证,并返回认证成功或失败的消息。

(3) password-publickey 认证:对于 SSH2 版本的客户端,要求同时进行 password 和 publickey 两种方式的认证,且只有两种认证均通过的情况下,才认为客户端身份认证通过;对于 SSH1 版本的客户端,只要通过其中任意一种认证即可。

(4) any 认证:不指定客户端的认证方式,客户端可采用 password 认证或 publickey 认证,且只要通过其中任何一种认证即可。

9.1.2　SSH 的层次

SSH 主要由三部分组成,即传输层协议[SSH-TRANS]、用户认证协议[SSH-USERAUTH]、连接协议[SSH-CONNECT]。

(1) 传输层协议[SSH-TRANS]:提供了服务器认证、保密性及完整性。此外,它有时还提供压缩功能。SSH-TRANS 通常运行在 TCP/IP 连接上,也可能用于其他可靠数据流上。SSH-TRANS 提供了强力的加密技术、密码主机认证及完整性保护。该协议中的

认证基于主机,并且该协议不执行用户认证。更高层的用户认证协议可以设计为在此协议之上。

(2) 用户认证协议[SSH-USERAUTH]:用于向服务器端提供客户端用户鉴别功能。它运行在传输层协议[SSH-TRANS]上面。当 SSH-USERAUTH 开始后,它从低层协议那里接收会话标识符(从第一次密钥交换中的交换哈希 H)。会话标识符唯一标识此会话并且适用于标记以证明私钥的所有权。SSH-USERAUTH 也需要知道低层协议是否提供保密性保护。

(3) 连接协议[SSH-CONNECT]:将多个加密隧道分成逻辑通道。它运行在用户认证协议上。它提供了交互式登录话路、远程命令执行、转发 TCP/IP 连接和转发 X11 连接。

9.1.3　SSH 的配置命令

表 9-1 所示是配置 SSH 时所需用到的一些命令。

表 9-1　SSH 的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
ssh server enable	开启 SSH 功能
public-key local create rsa	生成 RSA 密钥对
local-user name class manage	创建本地账户
password {simple|hash}******	设置密码
service-type ssh	设置服务类型为 SSH
user vty number	设置远程登录用户数
authentication-mode {scheme|none|password}	设置认证模式

实验 1　路由器开启 SSH 服务器端功能

实验目的:学会 SSH 的配置方法。

实验器材:H3C MSR36-20 三台。

实验要求:为三台路由器开启 SSH(Secure Shell,安全外壳)服务器端功能,对 SSH 用户采用 password 认证方式,用户名和密码为 000000。密码为明文类型,用户角色为 network-admin。客户端登录用户数为六人。

SSH 的配置拓扑图如图 9-1 所示。

实验步骤如下:

```
[R1]interface LoopBack 0
[R1-LoopBack0]ip address 9.9.9.1 32
```

认证基于主机，并且该协议不执行用户认证。更高层的用户认证协议可以设计为在此协议之上。

(2) 用户认证协议[SSH-USERAUTH]：用于向服务器端提供客户端用户鉴别功能。它运行在传输层协议[SSH-TRANS]上面。当 SSH-USERAUTH 开始后，它从低层协议那里接收会话标识符(从第一次密钥交换中的交换哈希 H)。会话标识符唯一标识此会话并且适用于标记以证明私钥的所有权。SSH-USERAUTH 也需要知道低层协议是否提供保密性保护。

(3) 连接协议[SSH-CONNECT]：将多个加密隧道分成逻辑通道。它运行在用户认证协议上。它提供了交互式登录话路、远程命令执行、转发 TCP/IP 连接和转发 X11 连接。

9.1.3 SSH 的配置命令

表 9-1 所示是配置 SSH 时所需用到的一些命令。

表 9-1 SSH 的配置命令

操作命令	操作说明
system-view	进入系统界面
ssh server enable	开启 SSH 功能
public-key local create rsa	生成 RSA 密钥对
local-user name class manage	创建本地账户
password {simple|hash}******	设置密码
service-type ssh	设置服务类型为 SSH
user vty number	设置远程登录用户数
authentication-mode {scheme|none|password}	设置认证模式

实验 1 路由器开启 SSH 服务器端功能

实验目的：学会 SSH 的配置方法。

实验器材：H3C MSR36-20 三台。

实验要求：为三台路由器开启 SSH(Secure Shell，安全外壳)服务器端功能，对 SSH 用户采用 password 认证方式，用户名和密码为 000000。密码为明文类型，用户角色为 network-admin。客户端登录用户数为六人。

SSH 的配置拓扑图如图 9-1 所示。

实验步骤如下：

```
[R1]interface LoopBack 0
[R1-LoopBack0]ip address 9.9.9.1 32
```

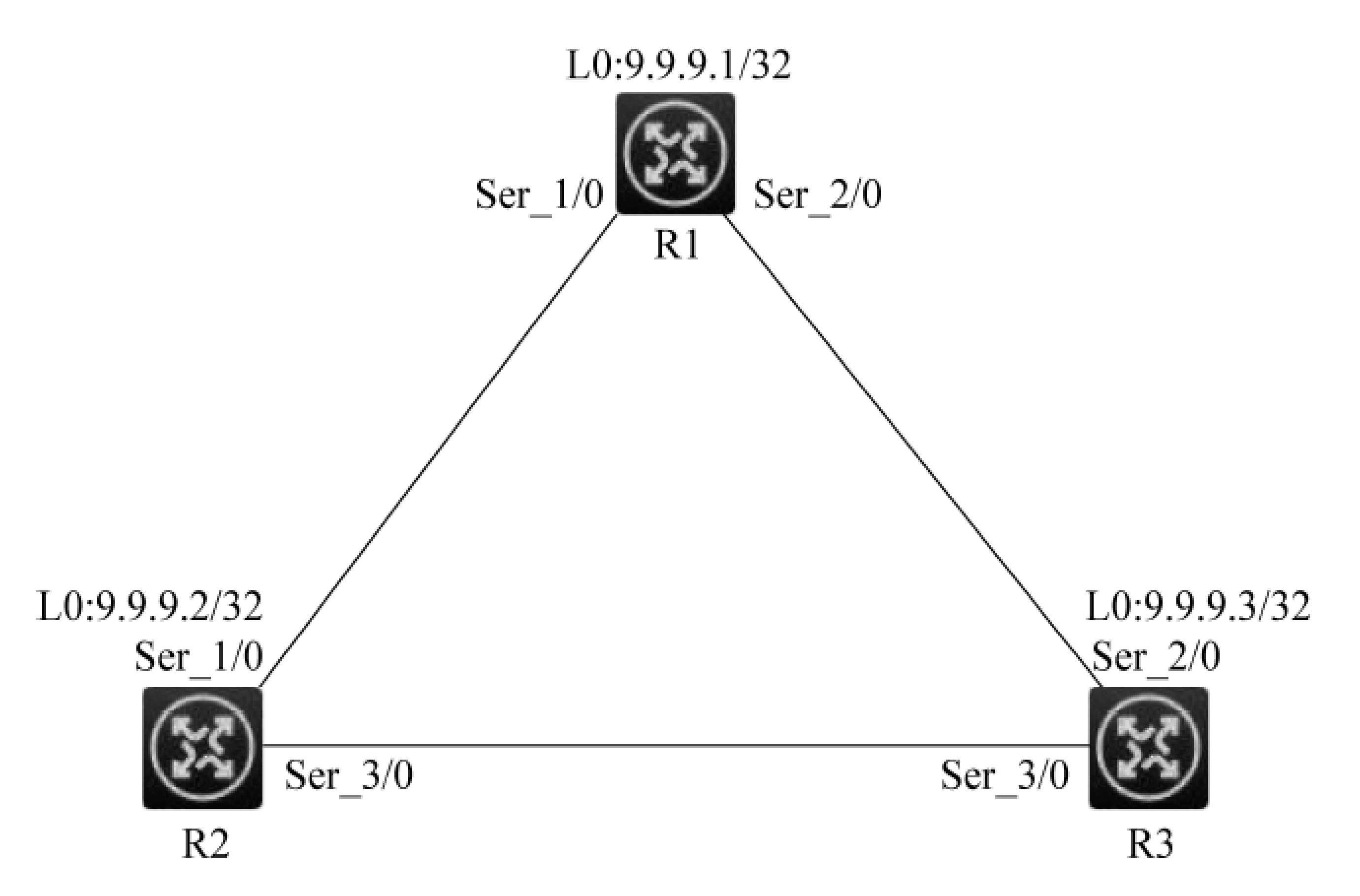


图 9-1 SSH 的配置拓扑图

```
[R1]ssh server enable
[R1]public-key local create rsa                        //生成 RSA 密钥对

[R1]local-user admin class manage                      //创建本地账户
[R1-luser-manage-admin]password simple admin           //设置密码
[R1-luser-manage-admin]authorization-attribute user-role network-admin
                                                       //设置权限
[R1-luser-manage-admin]service-type ssh                //设置服务类型
[R1-luser-manage-admin]quit
[R1]line vty 0 5                                       //设置远程登录用户数
[R1-line-vty0-5]authentication-mode scheme

[R2]interface LoopBack 0
[R2-LoopBack0]ip address 9.9.9.2 32
[R2]ssh server enable
[R2]public-key local create rsa                        //生成 RSA 密钥对
[R2]local-user admin class manage
[R2-luser-manage-admin]password simple admin
[R2-luser-manage-admin]authorization-attribute user-role network-admin
                                                       //设置权限
[R2-luser-manage-admin]service-type ssh                //设置服务类型
[R2-luser-manage-admin]quit
[R2]line vty 0 5                                       //设置远程登录用户数
[R2-line-vty0-5]authentication-mode scheme

[R3]interface LoopBack 0
[R3-LoopBack0]ip address 9.9.9.3 32
[R3]ssh server enable
[R3]public-key local create rsa                        //生成 RSA 密钥对
[R3]local-user admin class manage
[R3-luser-manage-admin]password simple admin
[R3-luser-manage-admin]authorization-attribute user-role network-admin
                                                       //设置权限
[R3-luser-manage-admin]service-type ssh                //设置服务类型
```

```
[R3-luser-manage-admin]quit
[R3]line vty 0 5                                    //设置远程登录用户数
[R3-line-vty0-5]authentication-mode scheme
```

实验结果如下：

在 R1 上查看。

```
[R1]display current-configuration
#
 version 7.1.075, Alpha 7571
#
 sysname R1
#
system-working-mode standard
xbar load-single
password-recovery enable lpu-type f-series
#vlan 1
#interface Serial1/0
#interface Serial2/0
#interface Serial3/0
#interface Serial4/0
#interface NULL0
#interface LoopBack0
 ip address 9.9.9.1 255.255.255.255
#interface GigabitEthernet0/0 port link-mode route
 combo enable copper
#interface GigabitEthernet0/1 port link-mode route
 combo enable copper
#interface GigabitEthernet0/2 port link-mode route
 combo enable copper
#interface GigabitEthernet5/0 port link-mode route
 combo enable copper
#interface GigabitEthernet5/1 port link-mode route
 combo enable copper
#interface GigabitEthernet6/0 port link-mode route
 combo enable copper
#interface GigabitEthernet6/1
port link-mode route combo enable copper
#scheduler logfile size 16
#line class aux
 user-role network-operator
#line class console
 user-role network-admin
#line class tty
 user-role network-operator
#line class vty
 user-role network-operator
#line aux 0
 user-role network-operator
#line con 0
```

```
 user-role network-admin
#line vty 0 5
 authentication-mode scheme
 user-role network-operator
#line vty 6 63
 user-role network-operator
#domain system
#domain default enable system
#role name level-0
 description Predefined level-0 role
#role name level-1
 description Predefined level-1 role
#role name level-2
 description Predefined level-2 role
#role name level-3
 description Predefined level-3 role
  //role name level-4 至 role name level-12 略
#role name level-13
 description Predefined level-13 role
#role name level-14
 description Predefined level-14 role
#user-group system
#local-user amdin class manage
password hash
$h$6$npOoLUwVlvX3868X$EdwLE88p7CeQNfzKXvDKBrb3H41xPCBfVNePr91XwJt+
ZCY7g21TKsQy+iL/BNtsZByCvJNUNQZAvPF1UPRbpA==
service-type ssh
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
# [R2]display current-configuration
#version 7.1.075, Alpha 7571
#sysname R2
#system-working-mode standard xbar load-single
 password-recovery enable
 lpu-type f-series
#vlan 1
#interface Serial1/0
#interface Serial2/0
#interface Serial3/0
#interface Serial4/0
#interface NULL0 interface LoopBack0
 ip address 9.9.9.2 255.255.255.255
#

#interface GigabitEthernet0/0 port link-mode route
 combo enable copper
#interface GigabitEthernet0/1 port link-mode route
 combo enable copper
#interface GigabitEthernet0/2 port link-mode route
```

```
  combo enable copper
#interface GigabitEthernet5/0 port link-mode route
  combo enable copper
#interface GigabitEthernet5/1 port link-mode route
  combo enable copper
#interface GigabitEthernet6/0 port link-mode route
  combo enable copper
#interface GigabitEthernet6/1 port link-mode route
  combo enable copper
#scheduler logfile size 16
#line class aux
  user-role network-operator
#line class console
  user-role network-admin
#line class tty
  user-role network-operator
#line class vty
  user-role network-operator
#line aux 0
  user-role network-operator
#line con 0
  user-role network-admin
#line vty 0 5
authentication-mode scheme
user-role network-operator
#line vty 6 63
  user-role network-operator
#ip route-static 0.0.0.0 0 Serial1/0
#ssh server enable
#domain system
#domain default enable system
#role name level-0
  description Predefined level-0 role
#//role name level-1
  description Predefined level-1 role
#
…
role name level-13
description Predefined level-13 role
#role name level-14
description Predefined level-14 role
#user-group system
#local-user admin class manage
password hash
$h$6$17ox0cPuRzVlUvKR$dl8+wSBazEtYS0ZL1I1ZTJGj3DzNuOrpjWljsBBtU4tDLSDiWxk77vtMf+qmD7t/
KSM8nAF3QybEqJAfQsNKnQ==
service-type ssh
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#
```

```
[R3]display current-configuration
#version 7.1.075, Alpha 7571
#sysname R2
#system-working-mode standard xbar load-single
 password-recovery enable
 lpu-type f-series
#vlan 1
#interface Serial1/0
#interface Serial2/0
#interface Serial3/0
#interface Serial4/0
#interface NULL0
#interface LoopBack0
 ip address 9.9.9.1 255.255.255.255
#

#interface GigabitEthernet0/0 port link-mode route
 combo enable copper
#interface GigabitEthernet0/1 port link-mode route
 combo enable copper
#interface GigabitEthernet0/2 port link-mode route
 combo enable copper
#interface GigabitEthernet5/0 port link-mode route
 combo enable copper
#interface GigabitEthernet5/1 port link-mode route
 combo enable copper
#interface GigabitEthernet6/0 port link-mode route
 combo enable copper
#interface GigabitEthernet6/1 port link-mode route
 combo enable copper
#scheduler logfile size 16
#line class aux
 user-role network-operator
#line class console
 user-role network-admin
#line class tty
 user-role network-operator
#line class vty
 user-role network-operator
#line aux 0
 user-role network-operator
#line con 0
 user-role network-admin
#line vty 0 5
authentication-mode scheme
user-role network-operator
#line vty 6 63
```

```
 user-role network-operator
#ssh server enable
#domain system
#domain default enable system
#role name level-0
 description Predefined level-0 role
#role name level-1
 description Predefined level-1 role
#
  //role name level-2
description Predefined level-2 role
#
…
role name level-12
description Predefined level-12 role
#role name level-13
 description Predefined level-13 role
#role name level-14
 description Predefined level-14 role
#user-group system
#local-user admin class manage
password hash
$h$6$l7ox0cPuRzVlUvKR$dl8+wSBazEtYS0ZLlI1ZTJGj3DzNuOrpjWljsBBtU4tDLSDiWxk77vtMf+qmD7t/
KSM8nAF3QybEqJAfQsNKnQ==
service-type ssh
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#
```

9.2 Telnet 简 介

Telnet 协议是 TCP/IP 协议簇中的一员，是 Internet 远程登录服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。在终端使用者的计算机上使用 Telnet 程序，用它连接到服务器。终端使用者可以在 Telnet 程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样，在本地就能控制服务器。要开始一个 Telnet 会话，必须输入用户名和密码登录服务器。Telnet 是常用的远程控制 Web 服务器的方法。

9.2.1 Telnet 的用途

Telnet 是 Internet 远程登录服务的标准协议和主要方式，最初由 ARPANet 开发，现在主要用于 Internet 会话，它的基本功能是允许用户登录进入远程主机系统。

Telnet 可以让我们坐在自己的计算机前通过 Internet 网络登录到另一台远程计算机

上，这台计算机可以是在隔壁的房间里，也可以是在地球的另一端。当登录上远程计算机后，本地计算机就等同于远程计算机的一个终端，我们可以用自己的计算机直接操纵远程计算机，享受远程计算机本地终端同样的操作权限。

Telnet 的主要用途就是使用远程计算机上所拥有的本地计算机没有的信息资源，如果远程的主要目的是在本地计算机与远程计算机之间传递文件，那么相比较而言使用 FTP 会更加快捷、有效。

9.2.2　安全隐患

虽然 Telnet 较为简单、实用、方便，但是在格外注重安全的现代网络技术中，Telnet 并不被重用。原因在于 Telnet 是一个明文传送协议，它将用户的所有内容，包括用户名和密码都明文在互联网上传送，具有一定的安全隐患，因此许多服务器都会选择禁用 Telnet 服务。如果我们要使用 Telnet 的远程登录，使用前应在远端服务器上检查并设置允许 Telnet 服务的功能。

9.2.3　Telnet 的交互过程

当我们使用 Telnet 登录进入远程计算机系统时，事实上启动了两个程序：一个是 Telnet 客户程序，运行在本地主机上；另一个是 Telnet 服务器程序，它运行在要登录的远程计算机上。本地主机上的 Telnet 客户程序主要完成以下功能：

- 建立与远程服务器的 TCP 连接；
- 从键盘上接收本地输入的字符；
- 将输入的字符串变成标准格式并传送给远程服务器；
- 从远程服务器接收输出的信息；
- 将该信息显示在本地主机屏幕上。

远程主机的“服务”程序通常被称为“精灵”，它平时不声不响地守候在远程主机上，一接到本地主机的请求，就会立马活跃起来，并完成以下功能：

- 通知本地主机，远程主机已经准备好了；
- 等候本地主机输入命令；
- 对本地主机的命令做出反应(如显示目录内容，或执行某个程序等)；
- 把执行命令的结果送回本地计算机中显示；
- 重新等候本地主机的命令。

在 Internet 中，很多服务都采取这样一种客户机/服务器结构。对使用者来讲，通常只要了解客户端的程序就可以了。

9.2.4　Telnet 的配置命令

表 9-2 所示是配置 Telnet 时所需用到的一些命令。

表 9-2 Telnet 的配置命令

操 作 命 令	操 作 说 明
system-view	进入系统界面
telnet server enable	开启 Telnet 服务
local-user name	建立本地用户
password {simple|hash} ******	设置密码
authorization-attribute level{number}	设置命令等级
service-type telnet	设置服务类型为 Telnet
user vty number	设置远程登录用户数
authentication-mode {scheme|none|password}	设置认证模式

实验 2 交换机开启 Telnet 功能

实验目的：学习并掌握 Telnet 的配置方法及如何使用。

实验要求：

（1）为交换机开启 Telnet 功能，对所有 Telnet 用户采用本地认证的方式。

（2）创建本地用户，设定用户名和密码均为 admin 的用户有三级命令权限。

开启交换机 Telnet 功能的配置拓扑图如图 9-2 所示。

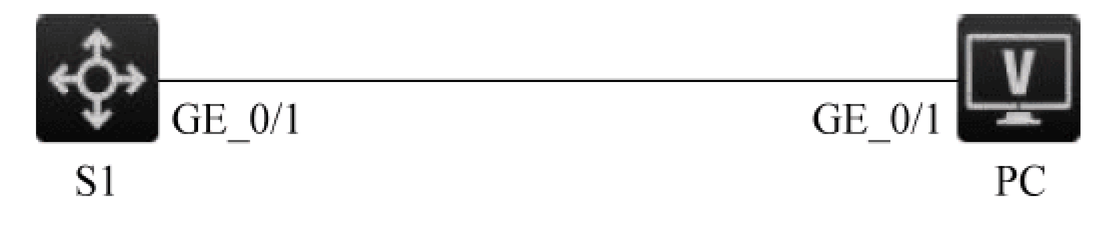


图 9-2 开启交换机 Telnet 功能的配置拓扑图

实验步骤如下：

```
[S1]int vlan 1
[S1-Vlan-interface1]ip address 192.168.0.55 24
[S1-Vlan-interface1]quit
[S1]telnet server en                                //开启 Telnet
[S1]local-user admin
[S1-luser-admin]password simple admin
[S1-luser-admin]authorization-attribute level 3     //设置命令等级
[S1-luser-admin]service-type telnet
[S1-luser-admin]user vty 0 4                        //设置五个用户可登录
[S1-ui-vty0-4]authentication-mode scheme
```

实验结果如图 9-3 所示。



图 9-3　交换机用 Telnet 登录并进入界面

实验 3　为路由器配置 Telnet

实验目的：学习并掌握 Telnet 的配置方法及如何使用。

实验器材：H3C MSR36-30 两台。

实验要求：为路由器开启 Telnet 功能，对所有 Telnet 用户采用本地认证的方式。创建本地用户，设定用户名和密码为 000000。且可在 R1 上登录 R2，也可在 R2 上登录 R1。

图 9-4 所示为路由器 Telnet 的配置拓扑图。



图 9-4　路由器 Telnet 的配置拓扑图

实验步骤如下：

```
[R1]interface Serial2/0
[R1-Serial2/0]ip address 10.10.10.1 24
[R1-Serial2/0]quit
[R1]telnet server enable                    //开启 Telnet 功能
[R1]local-user 000000
[R1-luser-manage-000000]password simple 000000
[R1-luser-manage-000000]service-type telnet  //设置服务类型为 Telnet
[R1-luser-manage-000000]user vty 0 4         //设置五个用户可登录
[R1-line-vty0-4]authentication-mode scheme   //设置认证方式为 scheme
[R1]ip route-static 192.168.1.1 24 Serial 2/0
  //设置静态路由，本例为 192.168.1.1 24
```

```
[R2]interface Serial2/0
[R2-Serial2/0]ip address 10.10.10.2 24
[R2-Serial2/0]quit
[R2]telnet server en
[R2]local-user 000000
[R2-luser-manage-000000]password simple 000000
[R2-luser-manage-000000]service-type telnet
[R2-luser-manage-000000]user vty 0 4
[R2-line-vty0-4]authentication-mode scheme
[R2-line-vty0-4]quit
[R2]ip route-static 0.0.0.0 0.0.0.0 Serial 2/0        //创建默认路由
```

实验结果如图 9-5 和图 9-6 所示，分别为 R1 和 R2 登入的效果。

```
<R1>telnet 10.10.10.2
Trying 10.10.10.2 ...
Press CTRL+K to abort
Connected to 10.10.10.2 ...

******************************************************************************
* Copyright (c) 2004-2016 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: 000000
Password:
<R2>
```

图 9-5　R1 登入的效果

```
<R2>telnet 10.10.10.1
Trying 10.10.10.1 ...
Press CTRL+K to abort
Connected to 10.10.10.1 ...

******************************************************************************
* Copyright (c) 2004-2016 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: 000000
Password:
<R1>
```

图 9-6　R2 登入的效果

9.3　SNMP 简　介

SNMP(Simple Network Management Protocol，简单网络管理协议)是互联网中的一种网络管理标准协议，广泛用于实现管理设备对被管理设备的访问和管理。

9.3.1 SNMP 的优势

支持网络设备的智能化管理。利用基于 SNMP 的网络管理平台,网络管理员可以查询网络设备的运行状态和参数,设置参数值,发现故障,完成故障诊断,进行容量规划和制作报告,支持对不同物理特性的设备进行管理。SNMP 只提供最基本的功能集,使得管理任务与被管理设备的物理特性和联网技术相对独立,从而实现对不同厂商设备的管理。

9.3.2 SNMP 的基本操作

SNMP 提供四种基本操作。

Get 操作:NMS 使用该操作查询 AgentMIB 中节点的值。

Set 操作:NMS 使用该操作设置 Agent MIB 中节点的值。

Trap 操作:Agent 使用该操作向 NMS 发送 Trap 报文。Agent 不要求 NMS 发送回应报文,NMS 也不会对 Trap 报文进行回应。SNMPv1、SNMPv2c 和 SNMPv3 均支持 Trap 操作。

Inform 操作:Agent 使用该操作向 NMS 发送 Inform 报文。Agent 要求 NMS 发送回应报文,因此,Inform 报文比 Trap 报文更可靠。如果 Agent 在一定时间内没有收到 NMS 的回应报文,则会启动重发机制。只有 SNMPv2c 和 SNMPv3 支持 Inform 操作。

9.3.3 SNMP 版本介绍

目前,设备运行于非 FIPS 模式时,支持 SNMPv1、SNMPv2c 和 SNMPv3 三种版本;设备运行于 FIPS 模式时,只支持 SNMPv3 版本。只有 NMS 和 Agent 使用的 SNMP 版本相同,NMS 才能和 Agent 建立连接。

SNMPv1 采用团体名(Community Name)认证机制。团体名类似于密码,用来限制 NMS 和 Agent 之间的通信。如果 NMS 设置的团体名和被管理设备上设置的团体名不同,则 NMS 和 Agent 不能建立 SNMP 连接,从而导致 NMS 无法访问 Agent,Agent 发送的告警信息也会被 NMS 丢弃。

SNMPv2c 也采用团体名认证机制。SNMPv2c 对 SNMPv1 的功能进行了扩展:提供了更多的操作类型;支持更多的数据类型;提供了更丰富的错误代码,能够更细致地区分错误。

SNMPv3 采用 USM(User-Based Security Model,基于用户的安全模型)认证机制。网络管理员可以设置认证和加密功能。认证用于验证报文发送方的合法性,避免非法用户的访问;加密则是对 NMS 和 Agent 之间的传输报文进行加密,以免被窃听。采用认证和加密功能可以为 NMS 和 Agent 之间的通信提供更高的安全性。

实验 4　路由器开启 SNMP

实验目的：掌握 SNMP 的配置方法。

实验器材：H3C MSR 36-20 三台。

实验要求：

（1）网管服务器只能通过 SNMPv3 访问设备。

（2）SNMP 组名和用户名都为 1234，认证算法为 md5，加密算法为 3des，认证密码和加密密码都是明文方式，密码是 12345678。

SNMP 的配置拓扑图如图 9-7 所示。

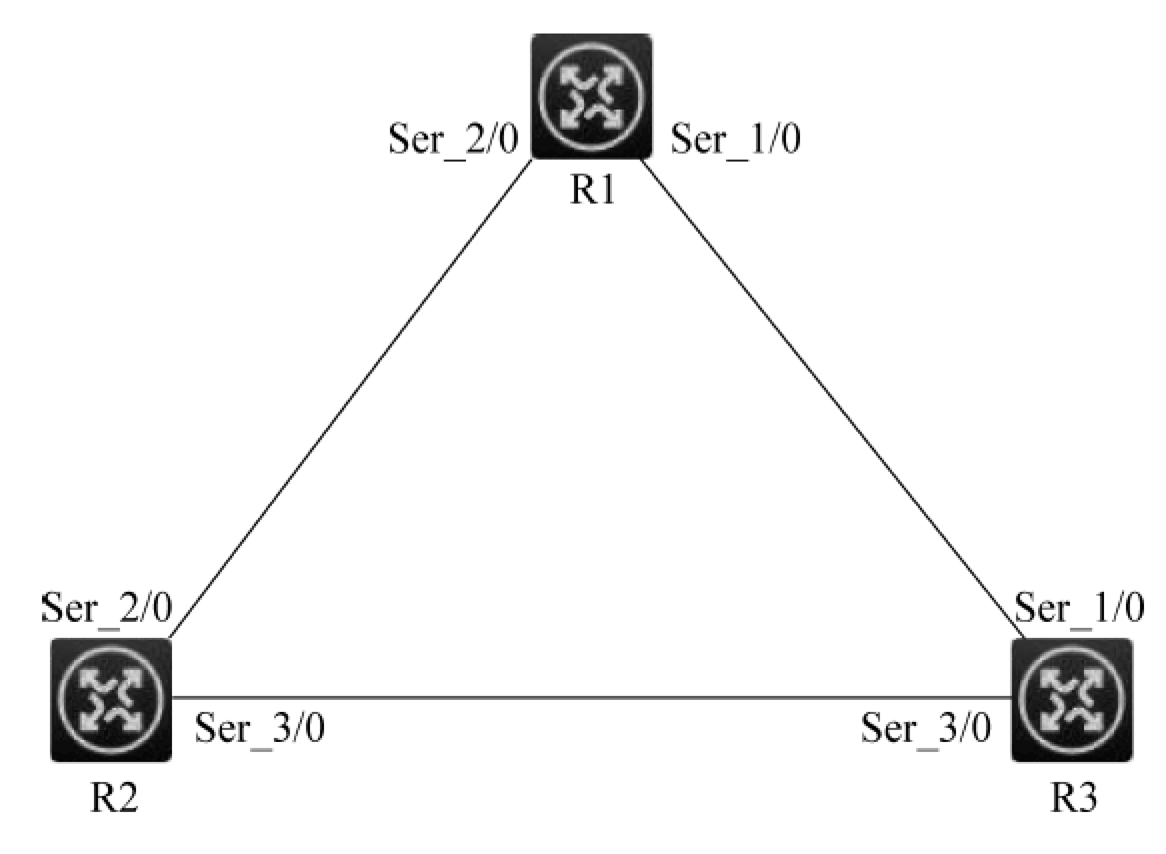


图 9-7　SNMP 的配置拓扑图

实验步骤如下：

```
[R1]snmp-agent usm-user v3 1234 1234 simple authentication-mode md5 1234
privacy-mode 3des 12345678
[R2]snmp-agent usm-user v3 1234 1234 simple authentication-mode md5 1234
privacy-mode 3des 12345678
[R3]snmp-agent usm-user v3 1234 1234 simple authentication-mode md5 1234
privacy-mode 3des 12345678
```

实验结果如下：

```
[R1]display snmp-agent usm-user
    Username: 1234
    Group name: 1234
        Engine ID: 800063A280487ADAFDFB6600000001
        Storage-type: nonVolatile
        UserStatus: active

[R2]display snmp-agent usm-user
Username: 1234
    Group name: 1234
```

```
        Engine ID: 800063A280487ADAFE022000000001
        Storage-type: nonVolatile
        UserStatus: active

 [R3]display snmp-agent usm-user
 Username: 1234
    Group name: 1234
        Engine ID: 800063A280487ADAFDFFC600000001
        Storage-type: nonVolatile
        UserStatus: active
```

项目 10　综 合 训 练

10.1　综合基础训练

项目背景：某知名外企进入我国，在北京建设了中国总部。为满足公司经营、管理的需要，现在建立公司信息化网络。总部办公区设有市场部、财务部、人力资源部、信息技术部四个部门，并在异地设立了一个分部。为了业务的开展，需要合作伙伴访问公司内部服务器。

公司规模在 2015 年快速发展，业务数据量和公司访问增长量巨大。为了更好地管理数据，提供服务，公司决定建立自己的小型数据中心，以达到快速、可靠交换数据的目的。

为适应公司业务需求，2016 年购入服务器并建立自己的系统服务平台。公司网络拓扑图如图 10-1 所示。

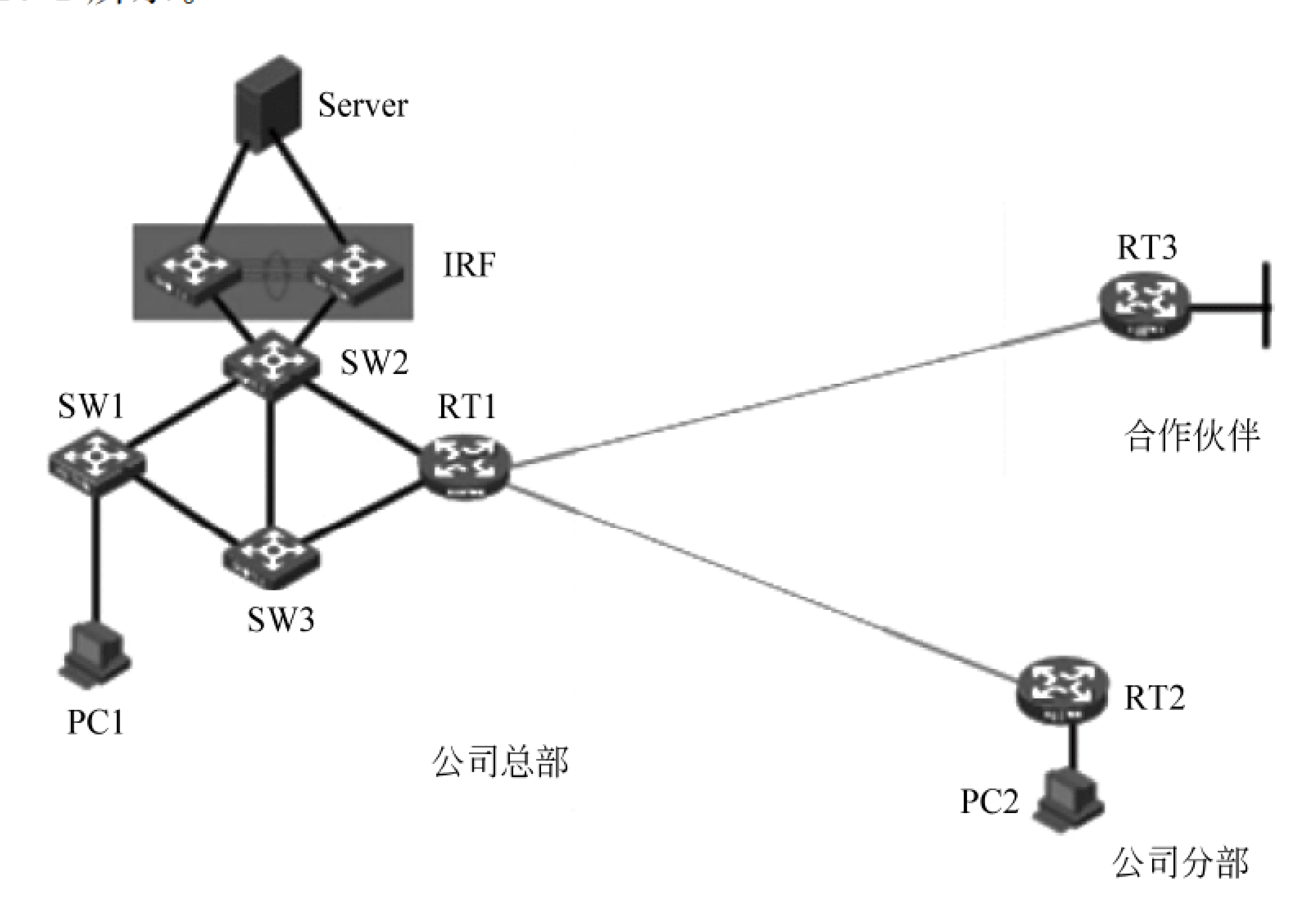


图 10-1　公司网络拓扑图

根据这个企业的建网需求，某系统集成公司进行网络规划和部署。为了确保部署成功，前期要进行仿真测试。测试环境包括三台路由器、三台以太网交换机、两台数据中心交换机、一台服务器、两台 PC。

1. 网络物理连接

首先根据如表 10-1 所示和图 10-1 的网络拓扑图,将所有网络设备与主机连接起来。

表 10-1 拓扑连接

源设备名称	设备接口	目标设备名称	设备接口
SW1	1 端口	SW2	2 端口
SW1	2 端口	SW3	2 端口
SW1	3 端口	PC1	
SW2	1 端口	RT1	以太网 0 端口
SW2	3 端口	SW3	3 端口
SW2	23 端口	IRF-SW1	23 端口
SW2	24 端口	IRF-SW2	24 端口
IRF-SW1	1 端口	Server(第一块网卡)	
IRF-SW2	1 端口	Server(第二块网卡)	
SW3	1 端口	RT1	以太网 1 端口
RT1	串口 2/0 端口	RT2	串口 2/0 端口
RT1	串口 3/0 端口	RT3	串口 2/0 端口
RT2	以太网 0 端口	PC2	

2. 网络设备配置

网络设备基本配置如表 10-2 所示。

表 10-2 网络设备基本配置

设备名称	配置主机名(Sysname 名)	说　明
SW1	SW1	总部二层交换机
SW2	SW2	总部三层交换机
SW3	SW3	总部三层交换机
IRF-SW1,IRF-SW2	IRF	总部数据中心交换机
RT1	RT1	总部路由器
RT2	RT2	分部路由器
RT3	RT3	合作伙伴路由器

3. 虚拟化配置

数据中心交换机需要实现虚拟化。交换机是 H3C 的 5800 系列交换机,所支持的虚拟化技术为 IRF。

在两台交换机上启用 IRF,要求为环形堆叠,IRF Domain 值为 10。

1. 网络物理连接

首先根据如表 10-1 所示和图 10-1 的网络拓扑图，将所有网络设备与主机连接起来。

表 10-1 拓扑连接

源设备名称	设备接口	目标设备名称	设备接口
SW1	1 端口	SW2	2 端口
SW1	2 端口	SW3	2 端口
SW1	3 端口	PC1	
SW2	1 端口	RT1	以太网 0 端口
SW2	3 端口	SW3	3 端口
SW2	23 端口	IRF-SW1	23 端口
SW2	24 端口	IRF-SW2	24 端口
IRF-SW1	1 端口	Server(第一块网卡)	
IRF-SW2	1 端口	Server(第二块网卡)	
SW3	1 端口	RT1	以太网 1 端口
RT1	串口 2/0 端口	RT2	串口 2/0 端口
RT1	串口 3/0 端口	RT3	串口 2/0 端口
RT2	以太网 0 端口	PC2	

2. 网络设备配置

网络设备基本配置如表 10-2 所示。

表 10-2 网络设备基本配置

设备名称	配置主机名(Sysname 名)	说　　明
SW1	SW1	总部二层交换机
SW2	SW2	总部三层交换机
SW3	SW3	总部三层交换机
IRF-SW1,IRF-SW2	IRF	总部数据中心交换机
RT1	RT1	总部路由器
RT2	RT2	分部路由器
RT3	RT3	合作伙伴路由器

3. 虚拟化配置

数据中心交换机需要实现虚拟化。交换机是 H3C 的 5800 系列交换机，所支持的虚拟化技术为 IRF。

在两台交换机上启用 IRF，要求为环形堆叠，IRF Domain 值为 10。

4. 链路可靠性配置

（1）广域网链路可靠性。RT1 与 RT2、RT1 与 RT3 使用广域网串口线连接，使用 PPP 协议。为了安全起见，使用双向 CHAP 验证（采用“用户名＋密码”的方式），验证口令为 123456。

（2）链路聚合。数据中心交换机与 SW2、数据中心交换机互联链路间采用动态链路聚合方式。

5. VLAN 配置

为了减少广播，需要规划 VLAN。具体要求如下。

（1）所有交换机之间均采用 Trunk 链路互联，要求配置合理，不允许不必要的 VLAN 通过。

（2）如表 10-3 所示，在二层交换机上完成 VLAN 配置和端口分配。

表 10-3　在二层交换机上完成 VLAN 配置和端口分配

VLAN 编号	VLAN 名称	说　明	端 口 分 配
VLAN 10	Marketing	市场部	SW1、IRF-SW1、IRF-SW2 上的 5～8 端口
VLAN 20	Finance	财务部	SW1、IRF-SW1、IRF-SW2 上的 9～12 端口
VLAN 30	HR	人力资源部	SW1、IRF-SW1、IRF-SW2 上的 13～16 端口
VLAN 100	IT	信息技术部	SW1、IRF-SW1、IRF-SW2 上的 17～20 端口
VLAN 400	Server	服务器区	IRF-SW1、IRF-SW2 上的 1～4 端口

（3）三层交换机与路由器间不建议采用 VLAN-Interface 接口互联，直接采用三层模式互联。

（4）IP 地址规划与配置北京总部办公区各部门以及公司分部信息点分布如表 10-4 所示。

表 10-4　信息点分布

部　门	信息点	部　门	信息点
市场部	100	信息技术部	13
财务部	40	公司分部	30
人力资源部	17		

由于公网地址紧张，所以只能在公司的总部和分部使用私网地址。计划使用 10.0.0.0/23 地址段。规划的结果如表 10-5 所示。

表 10-5　地址规划

区　域	IP 地址段	网　关
市场部	10.0.0.0/25	10.0.0.126
财务部	10.0.0.128/26	10.0.0.190

续表

区　域	IP 地址段	网　关
人力资源部	10.0.0.192/27	10.0.0.222
信息技术部	10.0.0.224/28	10.0.0.238
服务器区	10.0.1.96/28	10.0.1.110
公司分部	10.0.1.0/27	10.0.1.30

为了便于维护及管理，计划给公司内所有三层网络设备配置 LoopBack 地址，要求使用 32 位掩码。所规划的 LoopBack 地址如表 10-6 所示。

表 10-6　LoopBack 地址规划

设　备	IP 地址	设　备	IP 地址
RT1 的 LoopBack0 地址	9.9.9.1	SW3 的 LoopBack0 地址	9.9.9.3
SW2 的 LoopBack0 地址	9.9.9.2	RT2 的 LoopBack0 地址	9.9.9.4

此外，路由器间通过公网连接，其 IP 地址情况如表 10-7 所示。

表 10-7　IP 地址情况

设　备	IP 地址
RT1～RT2	202.0.1.0/30
RT1～RT3	202.0.2.0/30

公司内部设备间互联地址使用 172.16.0.0/24 网段，并使用 30 位掩码，如表 10-8 所示。

表 10-8　IP 地址使用情况

设　备	IP 地址	说　明
SW2～RT1	172.16.0.0/30	
SW3～RT1	172.16.0.4/30	

根据以上说明，请在设备上进行相关配置。

6. 路由配置

路由器之间的连接属于公网部分，使用静态路由。公司总部网络使用 OSPF 协议，分部使用静态路由，整体会达到互连互通。

OSPF 协议配置的具体要求如下。

(1) 总部网络配置为 OSPF 的骨干区域。

(2) 在 RT1 上配置去往分部的静态路由，并引入 OSPF 中。

(3) 配置 OSPF Hello 报文的发送时间为 1s。

(4) 配置 OSPF 进行 SPF 计算的时间间隔最小值为 100ms。

(5) 公司内部网络(包括公司分部)的所有网络设备均将 LoopBack 地址发布。

(6) 在交换机 SW1、SW2、SW3 上配置 MSTP,防止二层环路;在三层交换机 SW2 和 SW3 上配置 VRRP,实现主机的网关冗余。

网络配置的需求如下。

(1) 在正常情况下,部门内主机的数据流经由三层交换机 SW2～RT1 转发(不允许经由 SW3 转发);当 SW2 的上行链路发生故障时,主机的数据流切换到经 SW3～RT1 转发;故障恢复后,主机的数据流又能够切换回去。

(2) 各 VRRP 组中高优先级设置为 120,低优先级设置为 100。

(3) 为了增强网络的可靠性以适应数据中心快速收敛的要求,要求在相关设备上实现以下配置:

① DLDP。要求数据中心交换机与 SW2 的互联链路间使能 DLDP 协议,以防止由于单向链路引发的设备不能正常收发数据的情况。

② 链路聚合。要求链路聚合配置为动态(Dynamic)聚合组。

③ 设备安全访问设置。为网络设备开启远程登录(Telnet)功能,并按照表 10-9 为网络设备配置相应密码。并且只允许信息技术部的工作人员通过 Telnet 访问设备。

表 10-9　远程登录(Telnet)功能

设备名称(主机名)	远程登录密码	设备名称(主机名)	远程登录密码
RT1	000000(明文)	SW2	000000(明文)
RT2	000000(明文)	SW3	000000(明文)

10.2　综合提高训练

提示:本部分参考了全国职业技能大赛高职组计算机网络应用赛项赛题 C 卷中的部分试题。

项目背景:某集团公司在国内建立了总部,后来又在欧洲地区建立了分部。总部设有研发部、市场部、供应部、售后部四个部门,统一进行 IP 及业务资源的规划和分配。

集团规模在 2016 年快速发展,业务数据量和公司访问量增长巨大。为了更好地管理数据,提供服务,集团决定建立自己的小型数据中心及云计算服务平台,以达到快速、可靠交换数据以及增强业务部署弹性的目的。

集团总部及欧洲地区部的网络架设(实际设备)网络拓扑图如图 10-2 所示。其中,两台 S5800 交换机编号为 S4、S5,用于服务器高速接入;两台 S3600V2 编号为 S2、S3,作为总部的核心交换机;两台 MSR2630 路由器编号为 R2、R3,作为总部的核心路由器;一台 S3600V2 编号为 S1,作为接入交换机;一台 MSR2630 路由器编号为 R1,作为分支机构路由器。

请根据拓扑图及网络物理连接表完成设备的连线,如果现场已经提供的线缆不能满足需要,请现场制作所需线缆。相关设备及接口情况如表 10-10 所示。

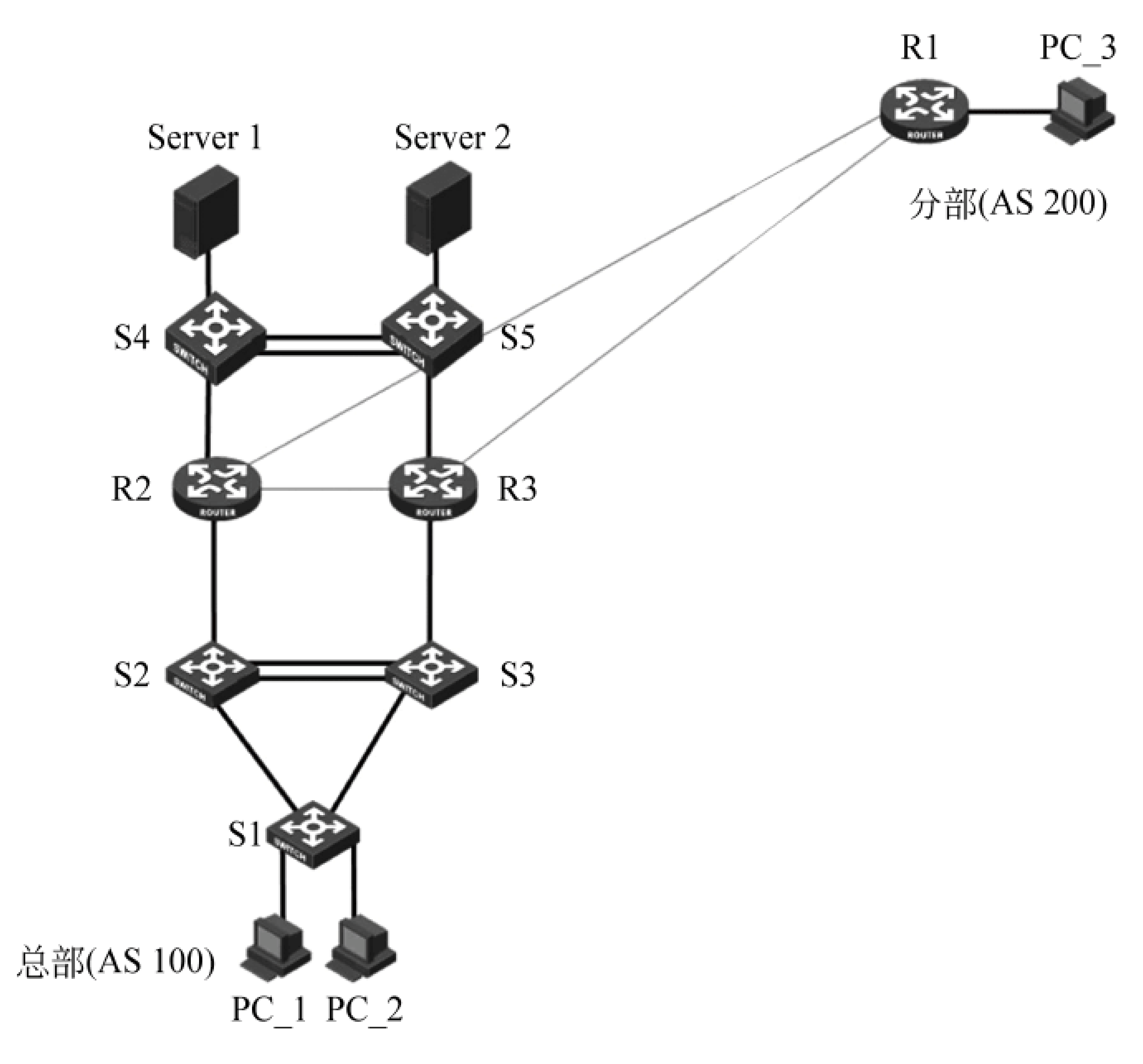


图 10-2 网络拓扑图

表 10-10 相关设备及接口

源设备名称	设备接口	目标设备名称	设备接口
S1	E1/0/1	PC_1	
S1	E1/0/2	PC_2	
S1	E1/0/23	S2	E1/0/1
S1	E1/0/24	S3	E1/0/1
S2	E1/0/2	S3	E1/0/2
S2	E1/0/3	S3	E1/0/3
S2	E1/0/4	R2	G0/0
S3	E1/0/4	R3	G0/0
R2	G0/1	S4	G1/0/1
R3	G0/1	S5	G1/0/1
S4	G1/0/2	S5	G1/0/2
S4	G1/0/3	S5	G1/0/3
S4	G1/0/4	Server 1	
S5	G1/0/4	Server 2	
R1	S2/0	R2	S2/0
R1	S3/0	R3	S2/0
R1	G0/0	PC_3	
R2	S3/0	R3	S3/0

1. 广域网链路配置

总部路由器与分部路由器间属于广域网链路，其中 R1～R2 所租用线路带宽为 2Mbps，R1～R3 所租用线路带宽为 1Mbps。R2～R3 线路带宽为 2Mbps。

请在路由器上进行相关配置，以使串口卡速率(波特率)能够匹配实际线路带宽。

2. PPP 部署

总部路由器与分部路由器间属于广域网链路。需要使用 PPP 进行安全保护。PPP 的具体要求如下。

(1) 使用 CHAP 协议。

(2) 总部路由器作为认证方(不配置用户名)，分部路由器作为被认证方。

(3) 用户名和密码均为 123456。

3. 虚拟局域网

为了减少广播，需要规划并配置 VLAN。具体要求如下。

(1) 配置合理，链路上不允许不必要 VLAN 的数据流通过。

(2) 交换机与路由器间的互联物理端口、S2 和 S3 间的 E1/0/3 端口、S4 和 S5 间的 G1/0/3 端口直接使用三层模式互联。

(3) 规划 S4 和 S5 交换机的 G1/0/4～G1/0/10 端口为连接服务器的端口；S2 和 S3 间的 E1/0/2 端口、S4 和 S5 间的 G1/0/2 端口为 Trunk 类型。

(4) 物理服务器属于 VLAN 100。

(5) 为隔离网络中部分终端用户间的二层互访，在交换机 S1 上使用 Isolate-user VLAN。VLAN 40 是 Isolate-user VLAN，VLAN 61～VLAN 64 是 Secondary VLAN。

根据上述信息，在交换机上完成 VLAN 配置和端口分配，如表 10-11 所示。

表 10-11 VLAN 配置和端口分配

设备	VLAN 编号	VLAN 名称	端　口	说　明
S1	VLAN 10	RD	E1/0/1～E1/0/4	研发部
	VLAN 20	Sales	E1/0/5～E1/0/8	市场部
	VLAN 30	Supply	E1/0/9～E1/0/12	供应部
	VLAN 40	Service		售后部
	VLAN 61		E1/0/13	Secondary VLAN
	VLAN 62		E1/0/14	Secondary VLAN
	VLAN 63		E1/0/15	Secondary VLAN
	VLAN 64		E1/0/16	Secondary VLAN

4. IPv4 地址部署

根据要求，为网络设备及 PC 分配 IPv4 地址，如表 10-12 所示。

表 10-12 IPv4 地址的分配

设备	接　　口	IPv4 地址
S2	VLAN 10	192.0.10.252/24
	VLAN 20	192.0.20.252/24
	VLAN 30	192.0.30.252/24
	VLAN 40	192.0.40.252/24
	E1/0/3	10.0.0.1/30
	E1/0/4	10.0.0.5/30
	LoopBack 0	9.9.9.202/32
S3	VLAN 10	192.0.10.253/24
	VLAN 20	192.0.20.253/24
	VLAN 30	192.0.30.253/24
	VLAN 40	192.0.40.253/24
	E1/0/3	10.0.0.2/30
	E1/0/4	10.0.0.9/30
	LoopBack 0	9.9.9.203/32
S4	VLAN 10	172.0.10.252/24
	VLAN 20	172.0.20.252/24
	VLAN 30	172.0.30.252/24
	VLAN 40	172.0.40.252/24
	VLAN 100	172.0.100.252/24
	G1/0/3	10.0.0.33/30
	G1/0/1	10.0.0.26/30
	LoopBack 0	9.9.9.204/32
S5	VLAN 10	172.0.10.253/24
	VLAN 20	172.0.20.253/24
	VLAN 30	172.0.30.253/24
	VLAN 40	172.0.40.253/24
	VLAN 100	172.0.100.253/24
	G1/0/3	10.0.0.34/30
	G1/0/1	10.0.0.30/30
	LoopBack 0	9.9.9.205/32
R1	S2/0	10.0.0.13/30
	S3/0	10.0.0.17/30
	G0/0	172.0.50.254/24
	LoopBack 0	9.9.9.1/32

续表

设备	接　　口	IPv4 地址
R2	G0/0	10.0.0.6/30
	G0/1	10.0.0.25/30
	S2/0	10.0.0.14/30
	S3/0	10.0.0.21/30
	LoopBack 0	9.9.9.2/32
R3	G0/0	10.0.0.10/30
	G0/1	10.0.0.29/30
	S2/0	10.0.0.18/30
	S3/0	10.0.0.22/30
	LoopBack 0	9.9.9.3/32
PC	PC1	自动获取
	PC2	192.0.10.101/24(网关为 192.0.10.254)
	PC3	172.0.50.101/24(网关为 172.0.50.254)

5. DHCP 中继

在交换机 S2、S3 上配置 DHCP 中继，对 VLAN 10 以内的用户进行中继，使得总部 PC1 用户使用 DHCP Relay 方式获取 IP 地址。具体要求如下。

(1) DHCP 服务器组编号为 0。

(2) DHCP 服务器 IP 地址为项目中的 Server1 上的 Windows 虚拟服务器地址 172.0.10.200。

6. IPv4 IGP 路由部署

因为历史性原因，总部使用 RIP、OSPF 多协议组网。S2、S3、R2、R3 规划使用 RIP 协议；S4、S5、R2、R3 规划使用 OSPF 协议。要求网络具有安全性、稳定性。具体要求如下。

(1) R2、R3 是边界路由器。

(2) RIP 进程号为 10，版本号为 RIP-2，取消自动聚合。

(3) OSPF 进程号为 10，区域为 0。

(4) 要求业务网段中不出现协议报文。

(5) 要求所有路由协议都发布具体网段。

(6) 为了管理方便，需要发布 LoopBack 地址，并尽量在 OSPF 域中发布。

(7) 优化 OSPF 相关配置，以尽量加快 OSPF 收敛。

(8) 不允许发布默认路由，也不允许使用静态路由。

7. IPv4 BGP 路由部署

总部与分部间使用 BGP 协议。具体要求如下：分部为 AS200，总部为 AS100；总部

内 R2、R3 需要建立 IBGP 连接;R2 上配置路由优先级值为 80;分部的所有路由必须通过 network 命令发布,总部路由通过引入方式发布;分部向总部发布默认路由,最终要求全网路由互通。

8. 路由优化部署

考虑到路由协议众多,且有引入路由的行为,为了防止本路由域内始发路由被再引回到本路由域,从而造成环路,规划在路由引入时使用 Route-Policy 进行过滤。具体要求如下。

(1) 采用给 IGP 路由打标签的方式实现。

(2) OSPF 路由引入后标签值为 60,BGP 路由引入后标签值为 250,RIP 路由引入后标签值为 120。

(3) 要求配置简单,实现合理。

9. 路由选路部署

考虑到从分部到总部有两条广域网线路,且其带宽不一样,所以规划 R1~R2 为主线路,R1~R3 为备线路。根据以上需求,在路由器上进行合理的路由协议配置。具体要求如下。

(1) BGP 协议只允许使用 Route-Policy 改变 MED 属性,且 MED 值必须为 100 或 200(如需要使用 ACL,则其编号值为 2020)。

(2) RIP 和 OSPF 通过路由引入时改变引入路由的 COST 值,且其值必须为 5 或 10。

10. PBR

考虑到分部到总部间有两条广域网线路,为合理利用带宽,规划从分部去往总部的 FTP 数据通过 R1~R2 的线路转发,从分部去往总部的 Web 数据通过 R1~R3 的线路转发。为达到上述目的,采用 PBR 实现。具体要求如下。

(1) Policy-based-route 编号为 1。

(2) 分部去往总部的 FTP 数据由 ACL3001 定义。

(3) 分部去往总部的 Web 数据由 ACL3002 定义。

11. MSTP 及 VRRP 部署

在总部交换机 S2、S3 上配置 MSTP,防止二层环路;要求所有数据流经过 S2 转发,S2 失效时经过 S3 转发。所配置的参数要求如下。

(1) region-name 为 H3C。

(2) 实例值为 1。

(3) S2 作为实例中的主根,S3 作为实例中的从根。

在 S2 和 S3 上配置 VRRP,实现主机的网关冗余。所配置的参数要求如表 10-13 所示。

表 10-13　S2 和 S3 的 VRRP 参数

VLAN	VRRP 备份组号(VRID)	VRRP 虚拟 IP
VLAN 10	10	192.0.10.254
VLAN 20	20	192.0.20.254
VLAN 30	30	192.0.30.254
VLAN 40	40	192.0.40.254

S2 作为所有主机的实际网关,S3 作为所有主机的备份网关,其中,各 VRRP 组中高优先级设置为 150,低优先级设置为 120。

在 S4 和 S5 上配置 VRRP,实现主机的网关冗余,所配置的参数要求如表 10-14 所示。

表 10-14　S4 和 S5 的 VRRP 参数

VLAN	VRRP 备份组号(VRID)	VRRP 虚拟 IP
VLAN 10	10	172.0.10.254
VLAN 20	20	172.0.20.254
VLAN 30	30	172.0.30.254
VLAN 40	40	172.0.40.254
VLAN 100	50	172.0.100.254

S4 作为所有主机的实际网关,S5 作为所有主机的备份网关,其中,各 VRRP 组中高优先级设置为 150,低优先级设置为 120。

12. QoS 部署

因总部与分部间的广域网带宽有限,为了保证关键的应用,需要在设备上配置 QoS,使分部与总部 DNS 服务器(172.0.20.200)之间的 DNS 数据流能够被加速转发,最大带宽为链路带宽的 10%。所配置的参数要求如下。

(1) ACL 编号为 3030(匹配 DNS 数据流)。

(2) Classifier 名称为 DNS。

(3) Behavior 名称为 DNS。

(4) QoS 策略名称为 DNS。

13. 设备与网络管理部署

根据要求,为网络设备配置主机名,如表 10-15 所示。

表 10-15　网络设备的名称

设备名称	配置主机名(Sysname 名)	说　　明
S1	S1	总部接入交换机
S2	S2	总部核心交换机 1
S3	S3	总部核心交换机 2

续表

设备名称	配置主机名(Sysname 名)	说　　明
S4	S4	总部数据中心交换机 1
S5	S5	总部数据中心交换机 2
R1	R1	分部路由器
R2	R2	总部路由器 1
R3	R3	总部路由器 2

为所有三层设备开启 ICMP 超时报文发送功能及 ICMP 目的不可达报文发送功能。

为路由器开启 SSH 服务器端功能，对 SSH 用户采用 password 认证方式，用户名和密码为 admin，密码为明文类型，用户角色为 network-admin。同时在线的最大 SSH 用户连接数为 10。

为交换机开启 Telnet 功能，对所有 Telnet 用户采用本地认证的方式。创建本地用户，设定用户名和密码为 admin 的用户有三级命令权限，用户名和密码为 000000 的用户有一级命令权限。密码为明文类型。

为路由器开启简单网络管理协议(SNMP)。要求网关服务器(172.0.100.200/24)只能通过 SNMPv3 访问设备，且用户只能读/写节点 snmp 下的对象。mib 对象名、SNMP 组名和用户名都为 2016，认证算法为 md5，加密算法为 3des，认证密码和加密密码都是明文方式，密码是 123456；当有 Trap 告警发生时，路由器会向网关服务器发送 Trap 报文。

要求只有网关服务器所在网段(172.0.100.0/24)的主机能够通过 SSH、Telnet、SNMP 来管理设备(如使用 ACL，则其编号要求为 2010)。

附录 1　项目 10 中综合基础训练部分的配置信息

1. 路由器 R1 的 display current-configuration 配置信息

```
[RT1]display current-configuration
#
  version 7.1.059, Release 0304P15
#
sysname RT1
#telnet server enable
telnet server acl 2000
#ospf 1
import-route static
spf-schedule-interval 1
area 0.0.0.0
network 9.9.9.1 0.0.0.0
network 9.9.9.2 0.0.0.0
network 9.9.9.3 0.0.0.0
network 9.9.9.4 0.0.0.0
#password-recovery enable
#vlan 1
#controller Cellular0/0
#interface Aux0
#interface Serial2/0
ppp authentication-mode chap domain system
ppp chap password cipher $c$3$nnbPgG4wOrJo8BL3cy8cKFdLj+JNr/PqJQ==
ppp chap user 123456
ip address 202.0.1.1 255.255.255.252
ospf timer hello 1
#interface Serial3/0
ppp authentication-mode chap domain system
ppp chap password cipher $c$3$1x0h2LtZWvwcbRYaEf7tReufvY2rJzFZkA==
ppp chap user 123456
ip address 202.0.2.1 255.255.255.252
ospf timer hello 1
#interface NULL0
#interface LoopBack0
ip address 9.9.9.1 255.255.255.255
#interface GigabitEthernet0/0 port link-mode route
#interface GigabitEthernet0/1 port link-mode route
```

```
#scheduler logfile size 16
#line class aux
  user-role network-admin
#line class tty
  user-role network-operator
#line class vty
  user-role network-operator
#line aux 0
  user-role network-admin
#line vty 0 4
  authentication-mode scheme
  user-role network-operator
#line vty 5 63
  user-role network-operator
#
ip route-static 10.0.1.0 27 202.0.1.2
#
acl basic 2000
rule 0 permit source 10.0.0.0 0.0.0.15
#domain sy
#domain system
authentication ppp local
#domain default enable system
#role name level-0
  description Predefined level-0 role
#role name level-1
  description Predefined level-1 role
#role name level-2
  description Predefined level-2 role
#role name level-3
  description Predefined level-3 role
#role name level-4
  description Predefined level-4 role
#role name level-5
  description Predefined level-5 role
#role name level-6
  description Predefined level-6 role
#role name level-7
  description Predefined level-7 role
#role name level-8
  description Predefined level-8 role
#role name level-9
  description Predefined level-9 role
#role name level-10
  description Predefined level-10 role
#role name level-11
  description Predefined level-11 role
#role name level-12
  description Predefined level-12 role
```

```
# role name level-13
  description Predefined level-13 role
# role name level-14
  description Predefined level-14 role
user-group system
#
local-user 000000 class manage
password hash
$h    $6    $EpDFqLISkkgzUS0C    $CWuREuVDU1UuYOdIC0QioxgAfThy926OSzIYGHXRfHvdNTj
FDxychEaDmI0pfD8lyYzNpMB3klTI/Cs/rdK3SA==
service-type telnet
authorization-attribute user-role network-operator
#
local-user 123456 class network
password cipher $c$3$ODT28IqrrM5kerUWHGrdc6V6ss4bhlGnkw==
service-type ppp
authorization-attribute user-role network-operator
#Return
```

2. 路由器 R2 的 display current-configuration 配置信息

```
[RT2]display current-configuration
#
version 7.1.059, Release 0304P15
#sysname RT2
#
telnet server enable
telnet server acl 2000
#password-recovery enable
#vlan 1
#controller Cellular0/0
#interface Aux0
#interface Serial2/0
ppp authentication-mode chap domain system
ppp chap password cipher $c$3$A/zdhtOkM6WYkxbGmzdyieJI9Ey10C7Cdw==
ppp chap user 123456
ip address 202.0.1.2 255.255.255.252
#interface Serial3/0
#interface NULL0

interface LoopBack0
ip address 9.9.9.4 255.255.255.255
#interface GigabitEthernet0/0 port link-mode route
#
interface GigabitEthernet0/1 port
  link-mode route
#scheduler logfile size 16
#line class aux
  user-role network-admin
```

```
#line class tty
  user-role network-operator
#line class vty
  user-role network-operator
#line aux 0
  user-role network-admin
#
line vty 0 4
authentication-mode scheme
user-role network-operator
#line vty 5 63
  user-role network-operator
#ip route-static 172.16.0.0 30 202.0.1.1
#acl basic 2000
rule 0 permit source 10.0.0.0 0.0.0.15
#domain system
authentication ppp local
#domain default enable system
#role name level-0
  description Predefined level-0 role
#role name level-1
  description Predefined level-1 role
#role name level-2
  description Predefined level-2 role
#role name level-3
  description Predefined level-3 role
#role name level-4
  description Predefined level-4 role
#role name level-5
  description Predefined level-5 role
#role name level-6
  description Predefined level-6 role
#role name level-7
  description Predefined level-7 role
#role name level-8
  description Predefined level-8 role
#role name level-9
  description Predefined level-9 role
#role name level-10
  description Predefined level-10 role
#role name level-11
  description Predefined level-11 role
#role name level-12
  description Predefined level-12 role
#role name level-13
  description Predefined level-13 role
#role name level-14
  description Predefined level-14 role
#user-group system
```

```
#local-user 000000 class manage
password hash
$h$6$9C24eD1Nldd0dmrg$gw5IIzXr6I9nQVlJBK5AKeVVFxRfXCkUfIAbs0DWCEnkgZvWd
BEu1N1L+h5W4uhCzQCZPeXX10rcUR6LoEVedw==
service-type telnet
authorization-attribute user-role network-operator
#
local-user 123456 class network
password cipher $c$3$z65zjU/rp7BtC55kMj9ZJQip3EjqQkj19Q==
service-type ppp
authorization-attribute user-role network-operator
#
return
```

3. 路由器 R3 的 display current-configuration 配置信息

```
[RT3]display current-configuration
#version 7.1.059, Release 0304P15
#sysname RT3
#password-recovery enable
#vlan 1
#controller Cellular0/0
#interface Aux0
#interface Serial2/0
ppp authentication-mode chap domain system
ppp chap password cipher $c$3$b1tUWrA2b5dzotnH62UZZuLvNB9RKkgz2w==
ppp chap user 123456
#interface Serial3/0
ip address 202.0.2.2 255.255.255.252
#interface NULL0
#interface GigabitEthernet0/0 port link-mode route
#interface GigabitEthernet0/1 port link-mode route
#scheduler logfile size 16
#line class aux
  user-role network-admin
#line class tty
  user-role network-operator
#line class vty
  user-role network-operator
#line aux 0
  user-role network-admin
#line vty 0 63
  user-role network-operator
#domain system
authentication ppp local
#domain default enable system
#role name level-0
  description Predefined level-0 role
#role name level-1
```

```
  description Predefined level-1 role
#role name level-2
  description Predefined level-2 role
#role name level-3
  description Predefined level-3 role
#role name level-4
  description Predefined level-4 role
#role name level-5
  description Predefined level-5 role
#role name level-6
  description Predefined level-6 role
#role name level-7
  description Predefined level-7 role
#role name level-8
  description Predefined level-8 role
#role name level-9
  description Predefined level-9 role
#role name level-10
  description Predefined level-10 role
#role name level-11
  description Predefined level-11 role
#role name level-12
  description Predefined level-12 role
#role name level-13
  description Predefined level-13 role
#role name level-14
  description Predefined level-14 role
#user-group system
#
local-user 000000 class manage
password hash
$h$6$9C24eD1Nldd0dmrg$gw5IIzXr6I9nQVlJBK5AKeVVFxRfXCkUfIAbs0DWCEnkgZvW
dBEu1N1L+h5W4uhCzQCZPeXXl0rcUR6LoEVedw==
service-type telnet
authorization-attribute user-role network-operator
#
local-user 123456 class network
password cipher $c$3$vopxZYhny3OX317qrCloz9zkIAY+njG3aQ==
service-type ppp
authorization-attribute user-role network-operator
#Return
```

4. 交换机 SW1 的 display current-configuration 配置信息

```
[SW1]display current-configuration
#
version 5.20, Release 2111P02
sysname SW1
#irf mac-address persistent timer irf auto-update enable
```

```
undo irf link-delay
#domain default enable system
#undo ip http enable
#password-recovery enable
#vlan 1
#vlan 10
  description 市场部
  name Marketing
#vlan 20
  description 财务部
  name Finance
#vlan 30
  description 人力资源部
  name HR
#vlan 100
  description 信息技术部
  name IT
#domain system
  access-limit disable state active
  idle-cut disable
  self-service-url disable
#user-group system
  group-attribute allow-guest
#stp region-configuration
  region-name H3C
  instance 1 vlan 10 20 30 100
  active region-configuration

  stp enable
#interface NULL0
#interface Vlan-interface1
ip address dhcp-alloc client-identifier mac Vlan-interface1
#interface Vlan-interface10
ip address 10.0.0.126 255.255.255.128
#interface Vlan-interface20
ip address 10.0.0.190 255.255.255.192
#interface Vlan-interface30
ip address 10.0.0.222 255.255.255.224
#interface Vlan-interface100
ip address 10.0.0.238 255.255.255.240
#interface Ethernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 100
#interface Ethernet1/0/2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
```

```
port trunk permit vlan 10 20 30 100
#interface Ethernet1/0/3 port link-mode bridge
#interface Ethernet1/0/4 port link-mode bridge
#interface Ethernet1/0/5 port link-mode bridge port access vlan 10
#interface Ethernet1/0/6 port link-mode bridge port access vlan 10
#interface Ethernet1/0/7 port link-mode bridge port access vlan 10
#interface Ethernet1/0/8 port link-mode bridge port access vlan 10
#interface Ethernet1/0/9 port link-mode bridge port access vlan 20
#interface Ethernet1/0/10 port link-mode bridge port access vlan 20
#interface Ethernet1/0/11 port link-mode bridge port access vlan 20
#interface Ethernet1/0/12 port link-mode bridge port access vlan 20
#interface Ethernet1/0/13 port link-mode bridge port access vlan 30
#interface Ethernet1/0/14 port link-mode bridge port access vlan 30
#interface Ethernet1/0/15 port link-mode bridge port access vlan 30
#interface Ethernet1/0/16 port link-mode bridge port access vlan 30
#interface Ethernet1/0/17 port link-mode bridge port access vlan 100
#interface Ethernet1/0/18 port link-mode bridge port access vlan 100
#interface Ethernet1/0/19 port link-mode bridge port access vlan 100
#interface Ethernet1/0/20 port link-mode bridge port access vlan 100
#interface Ethernet1/0/21 port link-mode bridge
#interface Ethernet1/0/22 port link-mode bridge
#interface Ethernet1/0/23 port link-mode bridge
#interface Ethernet1/0/24 port link-mode bridge
#interface GigabitEthernet1/0/25 port link-mode bridge
#interface GigabitEthernet1/0/26 port link-mode bridge
#interface GigabitEthernet1/0/27 port link-mode bridge
#interface GigabitEthernet1/0/28 port link-mode bridge
#load xml-configuration
#load tr069-configuration
#user-interface aux 0 user-interface vty 0 15
#
return
```

5. 交换机 SW2 的 display current-configuration 配置信息

```
[SW2]display current-configuration
#version 5.20, Release 2111P02
#sysname SW2
#irf mac-address persistent timer irf auto-update enable
  undo irf link-delay
#domain default enable system
#telnet server enable
#undo ip http enable
#password-recovery enable
#acl number 2000
rule 0 permit source 10.0.0.0 0.0.0.15
#vlan 1
#vlan 10
  description 市场部
```

```
  name Marketing
#vlan 20
  description 财务部
  name Finance
#vlan 30
  description 人力资源部
  name HR
#vlan 100
  description 信息技术部
  name IT
#domain system
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
#user-group system
  group-attribute allow-guest
#local-user 000000
password cipher $c$3$FJL3rTckIluc0kD4DEKKALWT9yRXBbb38A==
service-type telnet
#stp region-configuration
region-name H3C
instance 1 vlan 10 20 30 100
active region-configuration
#stp instance 1 root primary
stp enable
#interface Ethernet1/0/1
port link-mode route
ip address 172.16.0.6 255.255.255.252
#interface NULL0
#interface LoopBack0
ip address 9.9.9.3 255.255.255.255
#interface Vlan-interface1
ip address dhcp-alloc client-identifier mac Vlan-interface1
#interface Vlan-interface10
ip address 10.0.0.126 255.255.255.128
vrrp vrid 11 virtual-ip 10.0.0.126
#interface Vlan-interface20
ip address 10.0.0.190 255.255.255.192
vrrp vrid 21 virtual-ip 10.0.0.190
#interface Vlan-interface30
ip address 10.0.0.222 255.255.255.224
vrrp vrid 31 virtual-ip 10.0.0.222
#interface Vlan-interface100
ip address 10.0.0.238 255.255.255.240
vrrp vrid 101 virtual-ip 10.0.0.238
#interface Ethernet1/0/2
port link-mode bridge
port link-type trunk
```

```
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 100
#interface Ethernet1/0/3
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 100
#interface Ethernet1/0/4 port link-mode bridge
#interface Ethernet1/0/5 port link-mode bridge
port access vlan 10
#interface Ethernet1/0/6 port link-mode bridge
port access vlan 10
#interface Ethernet1/0/7 port link-mode bridge
port access vlan 10
#interface Ethernet1/0/8 port link-mode bridge
port access vlan 10
#interface Ethernet1/0/9 port link-mode bridge
port access vlan 20
#interface Ethernet1/0/10 port link-mode bridge
port access vlan 20
#interface Ethernet1/0/11 port link-mode bridge
port access vlan 20
#interface Ethernet1/0/12 port link-mode bridge
port access vlan 20
#interface Ethernet1/0/13 port link-mode bridge
port access vlan 30
#interface Ethernet1/0/14 port link-mode bridge
port access vlan 30
#interface Ethernet1/0/15 port link-mode bridge
port access vlan 30
#interface Ethernet1/0/16 port link-mode bridge
port access vlan 30
#interface Ethernet1/0/17 port link-mode bridge
port access vlan 100
#interface Ethernet1/0/18 port link-mode bridge
port access vlan 100
#interface Ethernet1/0/19 port link-mode bridge
port access vlan 100
#interface Ethernet1/0/20 port link-mode bridge
port access vlan 100
#interface Ethernet1/0/21 port link-mode bridge
#interface Ethernet1/0/22 port link-mode bridge
#
interface Ethernet1/0/23
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 100
port link-aggregation group 1
```

```
#interface Ethernet1/0/24
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 100
port link-aggregation group 1
#interface GigabitEthernet1/0/25 port link-mode bridge
#interface GigabitEthernet1/0/26 port link-mode bridge
#interface GigabitEthernet1/0/27 port link-mode bridge
#interface GigabitEthernet1/0/28 port link-mode bridge
#load xml-configuration
#load tr069-configuration
#user-interface aux 0 user-interface vty 0 4
acl 2000 inbound
authentication-mode scheme user-interface vty 5 15
#
return
```

6. 交换机 SW3 的 display current-configuration 配置信息

```
[SW3]display current-configuration
#
  version 5.20, Release 2111P02
#sysname SW3
#irf mac-address persistent timer irf auto-update enable
undo irf link-delay
#domain default enable system
#telnet server enable
#undo ip http enable
#password-recovery enable
#acl number 2000
rule 0 permit source 10.0.0.0 0.0.0.15
#vlan 1
#vlan 10
  description 市场部
  name Marketing
#vlan 20
  description 财务部
  name Finance
#vlan 30
  description 人力资源部
  name HR
#vlan 100
  description 信息技术部
  name IT
#domain system
access-limit disable state active
idle-cut disable
self-service-url disable
```

```
#user-group system
group-attribute allow-guest
#local-user 000000
password cipher $c$3$FJL3rTckIluc0kD4DEKKALWT9yRXBbb38A==
service-type telnet
#stp region-configuration
region-name H3C
instance 1 vlan 10 20 30 100
active region-configuration
#stp instance 1 root secondary
stp enable
#interface Ethernet1/0/1
port link-mode route
ip address 172.16.0.6 255.255.255.252
#interface NULL0
#interface LoopBack0
ip address 9.9.9.3 255.255.255.255
#interface Vlan-interface1
ip address dhcp-alloc client-identifier mac Vlan-interface1
#interface Vlan-interface10
ip address 10.0.0.126 255.255.255.128
vrrp vrid 11 virtual-ip 10.0.0.126
#interface Vlan-interface20
ip address 10.0.0.190 255.255.255.192
vrrp vrid 21 virtual-ip 10.0.0.190
#interface Vlan-interface30
ip address 10.0.0.222 255.255.255.224
vrrp vrid 31 virtual-ip 10.0.0.222
#interface Vlan-interface100
ip address 10.0.0.238 255.255.255.240
vrrp vrid 101 virtual-ip 10.0.0.238
#interface Ethernet1/0/2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 100
#interface Ethernet1/0/3
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 100
#interface Ethernet1/0/4 port link-mode bridge
#interface Ethernet1/0/5 port link-mode bridge
port access vlan 10
#interface Ethernet1/0/6 port link-mode bridge
port access vlan 10
#interface Ethernet1/0/7 port link-mode bridge
port access vlan 10
#interface Ethernet1/0/8 port link-mode bridge
```

```
port access vlan 10
#interface Ethernet1/0/9 port link-mode bridge
port access vlan 20
#interface Ethernet1/0/10 port link-mode bridge
port access vlan 20
#interface Ethernet1/0/11 port link-mode bridge
port access vlan 20
#interface Ethernet1/0/12 port link-mode bridge
port access vlan 20
#interface Ethernet1/0/13
port access vlan 30
#interface Ethernet1/0/14 port link-mode bridge
port access vlan 30
#interface Ethernet1/0/15 port link-mode bridge
port access vlan 30
#interface Ethernet1/0/16 port link-mode bridge
port access vlan 30
#interface Ethernet1/0/17 port link-mode bridge
port access vlan 100
#interface Ethernet1/0/18 port link-mode bridge
port access vlan 100
#interface Ethernet1/0/19 port link-mode bridge
port access vlan 100
#interface Ethernet1/0/20 port link-mode bridge
port access vlan 100
#interface Ethernet1/0/21
port link-mode bridge
#interface Ethernet1/0/22 port link-mode bridge
#interface Ethernet1/0/23 port link-mode bridge
#interface Ethernet1/0/24 port link-mode bridge
#interface GigabitEthernet1/0/25

#interface GigabitEthernet1/0/26 port link-mode bridge
#interface GigabitEthernet1/0/27 port link-mode bridge
#interface GigabitEthernet1/0/28 port link-mode bridge
#load xml-configuration
#load tr069-configuration
#user-interface aux 0 user-interface vty 0 4
acl 2000 inbound
authentication-mode scheme user-interface vty 5 15
#
return
```

7. 交换机 IRF 的 display current-configuration 配置信息

```
[irf]display current-configuration
#version 5.20, Release 1808P12
#sysname irf
#irf domain 10
```

```
irf mac-address persistent timer
irf auto-update enable
undo irf link-delay
#domain default enable system
#password-recovery enable
#vlan 1
#vlan 10
  description 说明
  name Marketing
#vlan 20
  description 财务部
  name Finance
#vlan 30
  description 人力资源部
  name HR
#vlan 100
  description 信息技术部
  name IT
#vlan 400
  description 服务器区
  name Server
#domain system
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
#user-group system
  group-attribute allow-guest
#interface Bridge-Aggregation1 link-aggregation mode dynamic
#interface NULL0
#interface Vlan-interface1
ip address dhcp-alloc client-identifier mac Vlan-interface1
#interface Vlan-interface10
ip address 10.0.0.126 255.255.255.128
#interface Vlan-interface20
ip address 10.0.0.190 255.255.255.192
#interface Vlan-interface30
ip address 10.0.0.222 255.255.255.224
#interface Vlan-interface100
ip address 10.0.0.238 255.255.255.240
#
interface Vlan-interface400
ip address 10.0.1.110 255.255.255.240
#interface GigabitEthernet1/0/1 port link-mode bridge
port access vlan 400
#interface GigabitEthernet1/0/2 port link-mode bridge
port access vlan 400
#interface GigabitEthernet1/0/3 port link-mode bridge
port access vlan 400
```

```
#interface GigabitEthernet1/0/4 port link-mode bridge
port access vlan 400
#interface GigabitEthernet1/0/5 port link-mode bridge
port access vlan 10
#interface GigabitEthernet1/0/6 port link-mode bridge
port access vlan 10
#interface GigabitEthernet1/0/7 port link-mode bridge
port access vlan 10
#interface GigabitEthernet1/0/8 port link-mode bridge
port access vlan 10
#interface GigabitEthernet1/0/9 port link-mode bridge
port access vlan 20
#interface GigabitEthernet1/0/10 port link-mode bridge
port access vlan 20
#interface GigabitEthernet1/0/11
port link-mode bridge
port access vlan 20
#
interface GigabitEthernet1/0/12 port link-mode bridge
port access vlan 20
#
interface GigabitEthernet1/0/13 port link-mode bridge
port access vlan 30
#interface GigabitEthernet1/0/14 port link-mode bridge
port access vlan 30
#interface GigabitEthernet1/0/15 port link-mode bridge
port access vlan 30
#interface GigabitEthernet1/0/16 port link-mode bridge
port access vlan 30
#interface GigabitEthernet1/0/17 port link-mode bridge
port access vlan 100
#interface GigabitEthernet1/0/18 port link-mode bridge
port access vlan 100
#interface GigabitEthernet1/0/19 port link-mode bridge
port access vlan 100
#interface GigabitEthernet1/0/20 port link-mode bridge port access vlan 100
#interface GigabitEthernet1/0/21 port link-mode bridge
#interface GigabitEthernet1/0/22 port link-mode bridge
#interface GigabitEthernet1/0/23 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 100 400
dldp enable
port link-aggregation group 1
#interface GigabitEthernet1/0/24 port link-mode bridge
#interface GigabitEthernet2/0/1 port link-mode bridge port access vlan 400
#interface GigabitEthernet2/0/2 port link-mode bridge port access vlan 400
#interface GigabitEthernet2/0/3 port link-mode bridge port access vlan 400
#interface GigabitEthernet2/0/4 port link-mode bridge port access vlan 400
```

```
#interface GigabitEthernet2/0/5 port link-mode bridge port access vlan 10
#interface GigabitEthernet2/0/6 port link-mode bridge port access vlan 10
#interface GigabitEthernet2/0/7 port link-mode bridge port access vlan 10
#interface GigabitEthernet2/0/8 port link-mode bridge port access vlan 10
interface GigabitEthernet2/0/9 port link-mode bridge port access vlan 20
#interface GigabitEthernet2/0/10 port link-mode bridge port access vlan 20
#interface GigabitEthernet2/0/11 port link-mode bridge port access vlan 20
#interface GigabitEthernet2/0/12 port link-mode bridge port access vlan 20
#interface GigabitEthernet2/0/13 port link-mode bridge port access vlan 30
#interface GigabitEthernet2/0/14 port link-mode bridge port access vlan 30
#interface GigabitEthernet2/0/15 port link-mode bridge port access vlan 30
#interface GigabitEthernet2/0/16 port link-mode bridge port access vlan 30
#
interface GigabitEthernet2/0/17 port link-mode bridge port access vlan 100
#interface GigabitEthernet2/0/18 port link-mode bridge port access vlan 100
#interface GigabitEthernet2/0/19 port link-mode bridge
port access vlan 100

interface GigabitEthernet2/0/20 port link-mode bridge port access vlan 100
#interface GigabitEthernet2/0/21 port link-mode bridge
#interface GigabitEthernet2/0/22 port link-mode bridge
#interface GigabitEthernet2/0/23 port link-mode bridge
#interface GigabitEthernet2/0/24
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 100 400
dldp enable
port link-aggregation group 1
#interface M-GigabitEthernet0/0/0
#interface Ten-GigabitEthernet1/0/25 port link-mode bridge
#interface Ten-GigabitEthernet1/0/27 port link-mode bridge
#interface Ten-GigabitEthernet1/0/28 port link-mode bridge
#interface Ten-GigabitEthernet2/0/25 port link-mode bridge
#interface Ten-GigabitEthernet2/0/27 port link-mode bridge
#interface Ten-GigabitEthernet2/0/28 port link-mode bridge
#interface Ten-GigabitEthernet1/0/26
#interface Ten-GigabitEthernet2/0/26
#load xml-configuration
#load tr069-configuration
#user-interface aux 0 1 user-interface vty 0 15
#irf-port 1/2
port group interface Ten-GigabitEthernet1/0/26 mode enhanced
#irf-port 2/1
port group interface Ten-GigabitEthernet2/0/26 mode enhanced
#return
```

附录 2　项目10中综合提高训练部分的配置信息

1. 路由器 R1 的 display current-configuration 配置信息

```
#version 7.1.059, Release 0304P15
#sysname R1
#ip unreachables enable ip ttl-expires enable
#password-recovery enable
#vlan 1
#traffic classifier DNS operator and
if-match acl 3030
#traffic behavior DNS
queue ef bandwidth pct 10 cbs-ratio 25
#qos policy DNS
classifier DNS behavior DNS
#policy-based-route 1 permit node 10
if-match acl 3001
apply output-interface Serial2/0
#policy-based-route 1 permit node 20
if-match acl 3002
apply output-interface Serial3/0
#controller Cellular0/0
#interface Aux0
#interface Serial2/0
ppp chap password cipher $c$3$HUUSlfT7tVTtfuo3RjQ3Vuex+wYOpitqYg==
ppp chap user 123456
ip address 10.0.0.13 255.255.255.252
qos apply policy DNS outbound

#interface Serial3/0 ppp chap password cipher $c$3$bKPW5YLJq9zA01LurCTSZ Uv9Bfq2wJzK3Q=
=
ppp chap user 123456
ip address 10.0.0.17 255.255.255.252
qos apply policy DNS outbound
#interface NULL0
#interface LoopBack0
ip address 9.9.9.1 255.255.255.255
#interface GigabitEthernet0/0 port link-mode route
ip address 172.0.50.254 255.255.255.0
ip policy-based-route 1
```

```
#interface GigabitEthernet0/1 port link-mode route
#bgp 200
router-id 9.9.9.1
peer 10.0.0.14 as-number 100
peer 10.0.0.14 connect-interface Serial2/0
peer 10.0.0.18 as-number 100
peer 10.0.0.18 connect-interface Serial3/0
#address-family ipv4 unicast
network 9.9.9.1 255.255.255.255
network 10.0.0.12 255.255.255.252
network 10.0.0.16 255.255.255.252
network 172.0.50.0 255.255.255.0
peer 10.0.0.14 enable
peer 10.0.0.14 default-route-advertise
peer 10.0.0.18 enable
peer 10.0.0.18 default-route-advertise
#scheduler logfile size 16
#line class aux
  user-role network-admin
#line class tty
  user-role network-operator
#line class vty
  user-role network-operator
#line aux 0
  user-role network-admin
#line vty 0 63
  authentication-mode scheme
  user-role network-admin user-
  role network-operator
#snmp-agent
snmp-agent local-engineid 800063A2803A7CABE4010500000001
snmp-agent sys-info version v3
snmp-agent target-host trap address udp-domain 172.0.100.200 params securityname
2016 v3 privacy
snmp-agent mib-view included 2016 snmp
snmp-agent usm-user v3 2016 2016 cipher authentication-mode md5
$c$3$HNj2VfAJ1CXoA2ScRCMwAfNvWc3zChHTU0e06gCioXyzmA==privacy-mode 3des
$c$3$0un3VdiWxVEXSfirm+hMOiy5Fj4VpSfRdSeb87ao/1ZY+XqEDHXwqRjkoNOVVAGImX8=acl
2010
snmp-agent trap enable arp
snmp-agent trap enable radius
#ssh server enable
ssh user admin service-type all authentication-type password
ssh server acl 2010
#acl basic 2010
rule 0 permit source 172.0.100.0 0.0.0.255
#acl advanced 3001
rule 10 permit tcp destination-port eq ftp
rule 20 permit tcp destination-port eq ftp-data
```

```
#acl advanced 3002
rule 10 permit tcp destination-port eq www
#acl advanced 3030
rule 10 permit udp source 172.0.50.0 0.0.0.255 destination 172.0.20.200 0 destination-port
eq dns
#domain system
#aaa session-limit ssh 10 domain default enable system
#role name level-0
  description Predefined level-0 role
#role name level-1
  description Predefined level-1 role
#role name level-2
  description Predefined level-2 role
#role name level-3
  description Predefined level-3 role
#role name level-4
  description Predefined level-4 role
#role name level-5
  description Predefined level-5 role
#role name level-6
  description Predefined level-6 role
#role name level-7
  description Predefined level-7 role
#role name level-8
  description Predefined level-8 role
#role name level-9
  description Predefined level-9 role
#role name level-10
  description Predefined level-10 role
#role name level-11
  description Predefined level-11 role
#role name level-12
  description Predefined level-12 role
#role name level-13
  description Predefined level-13 role
#role name level-14
  description Predefined level-14 role
#user-group system
#local-user admin class manage
password hash
$h$6$11XfdA/kSLgEjW+u$E7fWggCG9tjpkWNx6Jzj38BaTgqXu129705v2XOWTzLwg XfDN5sJ+eCx1
YOGRD8AatbzJDW+mFW6u362cFP/2A==
service-type ssh
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#return
```

2. 路由器 R2 的 display current-configuration 配置信息

```
#version 7.1.059, Release 0304P15
```

```
#sysname R2
#ospf 10 router-id 9.9.9.2
import-route rip 10 cost 5 tag 120 route-policy import
import-route bgp cost 5 tag 250 route-policy import silent-interface Serial2/0
spf-schedule-interval 1
area 0.0.0.0
network 9.9.9.2 0.0.0.0
network 10.0.0.12 0.0.0.3
network 10.0.0.20 0.0.0.3
network 10.0.0.24 0.0.0.3
#rip 10
undo summary
version 2
network 10.0.0.4 0.0.0.3
import-route ospf 10 cost 5 route-policy import tag 60
import-route bgp cost 5 route-policy import tag 250
#ip unreachables enable ip ttl-expires enable
#password-recovery enable
#vlan 1
#traffic classifier DNS operator and
if-match acl 3030
#traffic behavior DNS
queue ef bandwidth pct 10 cbs-ratio 25
#qos policy DNS
classifier DNS behavior DNS
#controller Cellular0/0
#interface Aux0
#interface Serial2/0
ppp authentication-mode chap
ip address 10.0.0.14 255.255.255.252
qos apply policy DNS outbound
#interface Serial3/0
ip address 10.0.0.21 255.255.255.252
ospf timer hello 1
ospf network-type p2p
ospf bfd enable
#interface NULL0
#interface LoopBack0
ip address 9.9.9.2 255.255.255.255
#interface GigabitEthernet0/0 port link-mode route
ip address 10.0.0.6 255.255.255.252
#interface GigabitEthernet0/1 port link-mode route
ip address 10.0.0.25 255.255.255.252
ospf timer hello 1
ospf network-type p2p
ospf bfd enable
#bgp 100
router-id 9.9.9.2
peer 9.9.9.3 as-number 100
```

```
peer 9.9.9.3 connect-interface LoopBack0
peer 10.0.0.13 as-number 200
#address-family ipv4 unicast
preference 80 80 80
import-route direct
import-route rip 10 route-policy import
import-route ospf 10 route-policy import
peer 9.9.9.3 enable
peer 9.9.9.3 next-hop-local
peer 10.0.0.13 enable
peer 10.0.0.13 route-policy export export
#route-policy export permit node 10
if-match ip address acl 2020
apply cost 100
#route-policy import deny node 10
if-match tag 60
#route-policy import deny node 20
if-match tag 250
#route-policy import deny node 30
if-match tag 120
#route-policy import permit node 40
#scheduler logfile size 16
#line class aux
  user-role network-admin
#line class tty
  user-role network-operator
#line class vty
  user-role network-operator
#line aux 0
  user-role network-admin
#line vty 0 63
  authentication-mode scheme
  user-role network-admin user-
  role network-operator
#snmp-agent
snmp-agent local-engineid 800063A2803A7CABE4010500000001
snmp-agent sys-info version v3
snmp-agent target-host trap address udp-domain 172.0.100.200 params securityname
2016 v3 privacy
snmp-agent mib-view included 2016 snmp
snmp-agent usm-user v3 2016 2016 cipher authentication-mode md5
$c$3$HNj2VfAJ1CXoA2ScRCMwAfNvWc3zChHTU0e06gCioXyzmA==privacy-mode 3des
$c$3$0un3VdiWxVEXSfirm+hMOiy5Fj4VpSfRdSeb87ao/1ZY+XqEDHXwqRjkoNOVVAGImX8=
acl
2010
snmp-agent trap enable arp
snmp-agent trap enable radius
#ssh server enable
ssh user admin service-type all authentication-type password
```

```
ssh server acl 2010
#acl basic 2010
rule 0 permit source 172.0.100.0 0.0.0.255
#acl basic 2020
rule 0 permit
#acl advanced 3030
rule 10 permit udp source 172.0.20.200 0 destination 172.0.50.0 0.0.0.255 source-port eq dns
#domain system
#aaa session-limit ssh 10 domain default enable system
#role name level-0
  description Predefined level-0 role
#role name level-1
  description Predefined level-1 role
#role name level-2
  description Predefined level-2 role
#role name level-3
  description Predefined level-3 role
#role name level-4
  description Predefined level-4 role
#role name level-5
  description Predefined level-5 role
#role name level-6
  description Predefined level-6 role
#role name level-7
  description Predefined level-7 role
#role name level-8
  description Predefined level-8 role
#role name level-9
  description Predefined level-9 role
#role name level-10
  description Predefined level-10 role
#role name level-11
  description Predefined level-11 role
#role name level-12
  description Predefined level-12 role
#role name level-13
  description Predefined level-13 role
#role name level-14
  description Predefined level-14 role
#user-group system
#local-user admin class manage
password hash
$h $6 $FAYY52V/Hr3Q8FbA $/g/nolljyIGnS22qsI16DbKg3xvkk7XnOHKwZnkeEvdPsaUqOJ + Rt2pzi
hAVUNI2HN327440FPVmzY4iy8Hqqw==
service-type ssh
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#local-user 123456 class network
password cipher $c$3$XVu+TC++2ejqJv9QxwQsNfQIZLuJo4PzCA==
```

```
service-type ppp
authorization-attribute user-role network-operator
#return
```

3. 路由器 R3 的 display current-configuration 配置信息

```
#version 7.1.059, Release 0304P15
#sysname R3
#ospf 10 router-id 9.9.9.3
import-route rip 10 cost 10 tag 120 route-policy import
import-route bgp cost 10 tag 250 route-policy import silent-interface Serial2/0
spf-schedule-interval 1
area 0.0.0.0
network 9.9.9.3 0.0.0.0
network 10.0.0.16 0.0.0.3
network 10.0.0.20 0.0.0.3
network 10.0.0.28 0.0.0.3
#rip 10
undo summary
version 2
network 10.0.0.8 0.0.0.3
import-route ospf 10 cost 10 route-policy import tag 60
import-route bgp cost 10 route-policy import tag 250
#ip unreachables enable ip ttl-expires enable
#password-recovery enable
#vlan 1
#traffic classifier DNS operator and
if-match acl 3030
#traffic behavior DNS
queue ef bandwidth pct 10 cbs-ratio 25
#qos policy DNS
classifier DNS behavior DNS
#controller Cellular0/0
#interface Aux0
#interface Serial2/0
ppp authentication-mode chap
ip address 10.0.0.18 255.255.255.252
qos apply policy DNS outbound
#interface Serial3/0
ip address 10.0.0.22 255.255.255.252
ospf timer hello 1
ospf network-type p2p
ospf bfd enable
#interface NULL0
#interface LoopBack0
ip address 9.9.9.3 255.255.255.255
#interface GigabitEthernet0/0 port link-mode route
ip address 10.0.0.10 255.255.255.252
#interface GigabitEthernet0/1 port link-mode route
```

```
ip address 10.0.0.29 255.255.255.252
ospf timer hello 1
ospf network-type p2p
ospf bfd enable
#bgp 100
router-id 9.9.9.3
peer 9.9.9.2 as-number 100
peer 9.9.9.2 connect-interface LoopBack0
peer 10.0.0.17 as-number 200
#address-family ipv4 unicast
import-route direct
import-route rip 10 route-policy import
import-route ospf 10 route-policy import
peer 9.9.9.2 enable
peer 9.9.9.2 next-hop-local
peer 10.0.0.17 enable
peer 10.0.0.17 route-policy export export
#route-policy export permit node 10
if-match ip address acl 2020
apply cost 200
#route-policy import deny node 10
if-match tag 60
#route-policy import deny node 20
if-match tag 250
#route-policy import deny node 30
if-match tag 120
#route-policy import permit node 40
#scheduler logfile size 16
#line class aux
  user-role network-admin
#line class tty
  user-role network-operator
#line class vty
  user-role network-operator
#
line aux 0
user-role network-admin
#line vty 0 63
authentication-mode scheme user-role network-admin user-role network-operator
#snmp-agent
snmp-agent local-engineid 800063A2803A7CABE4010500000001
snmp-agent sys-info version v3
snmp-agent target-host trap address udp-domain 172.0.100.200 params securityname
2016 v3 privacy
snmp-agent mib-view included 2016 snmp
snmp-agent usm-user v3 2016 2016 cipher authentication-mode md5
$c$3$HNj2VfAJ1CXoA2ScRCMwAfNvWc3zChHTU0e06gCioXyzmA==privacy-mode 3des
$c$3$0un3VdiWxVEXSfirm+hMOiy5Fj4VpSfRdSeb87ao/1ZY+XqEDHXwqRjkoNOVVAGImX8=acl
2010
```

```
snmp-agent trap enable arp
snmp-agent trap enable radius
#ssh server enable
ssh user admin service-type all authentication-type password
ssh server acl 2010
#acl basic 2010
rule 0 permit source 172.0.100.0 0.0.0.255
#acl basic 2020
rule 0 permit
#acl advanced 3030
rule 10 permit udp source 172.0.20.200 0 destination 172.0.50.0 0.0.0.255 source-port eq dns
#domain system
#aaa session-limit ssh 10 domain default enable system
#role name level-0
  description Predefined level-0 role
#role name level-1
  description Predefined level-1 role
#role name level-2
  description Predefined level-2 role
#role name level-3
  description Predefined level-3 role
#role name level-4
  description Predefined level-4 role
#role name level-5
  description Predefined level-5 role
#role name level-6
  description Predefined level-6 role
#role name level-7
  description Predefined level-7 role
#role name level-8
  description Predefined level-8 role
#role name level-9
  description Predefined level-9 role
#role name level-10
  description Predefined level-10 role
#role name level-11
  description Predefined level-11 role
#role name level-12
  description Predefined level-12 role
#role name level-13
  description Predefined level-13 role
#role name level-14
  description Predefined level-14 role
#user-group system
local-user admin class manage
password hash
$h  $6  $kyLq0xkG9LpXJ81x  $7XdQfHjEyQvBLpy06wMNoMHtF7  +  lWf  +  qik8AbYcFPsiKb3
BZh2kKGyX2G4kOLtRTqvUePXuVk+Xt3Tmx4tDRZg==
service-type ssh
```

```
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#local-user 123456 class network
password cipher $c$3$hJAXEhFUrnr47kFj7bhDM8QbqMEhsqbARQ==
service-type ppp
authorization-attribute user-role network-operator
#return
```

4. 交换机 S1 的 display current-configuration 配置信息

```
#version 5.20, Release 2108P01
#sysname S1
#irf mac-address persistent timer irf auto-update enable
undo irf link-delay
#domain default enable system
#telnet server enable
#undo ip http enable
#password-recovery enable
#vlan 1
#vlan 10
description 研发部
name RD
vlan 20
description 市场部
name Sales
#vlan 30
description 供应部
name Supply
#vlan 40
description 售后部
name Service
isolate-user-vlan enable
#vlan 61
description Secondary VLAN
#vlan 62
description Secondary VLAN
#vlan 63
description Secondary VLAN
#vlan 64
description Secondary VLAN
#domain system
access-limit disable
state active
  idle-cut disable
  self-service-url disable
#user-group system
group-attribute allow-guest
#local-user 000000
password cipher $c$3$VuB/beP6uink6lDXUrMRBZsEf06t9LkOkA==
```

```
authorization-attribute level 1
service-type telnet local-user admin
password cipher $c$3$9pmym2OewAVyjgu2JMSuDJY30Cihv4QR
authorization-attribute level 3
service-type telnet
#stp region-configuration
region-name H3C
instance 1 vlan 10 20 30 40 61 to 64
active region-configuration
#stp enable
#interface NULL0
#interface Vlan-interface1
ip address dhcp-alloc client-identifier mac Vlan-interface1
#interface Ethernet1/0/1 port link-mode bridge
port access vlan 10
#interface Ethernet1/0/2 port link-mode bridge
port access vlan 10
#interface Ethernet1/0/3 port link-mode bridge
port access vlan 10
#interface Ethernet1/0/4 port link-mode bridge
port access vlan 10
#interface Ethernet1/0/5 port link-mode bridge
port access vlan 20
#interface Ethernet1/0/6 port link-mode bridge
port access vlan 20
#interface Ethernet1/0/7 port link-mode bridge
port access vlan 20
#interface Ethernet1/0/8 port link-mode bridge
port access vlan 20
#interface Ethernet1/0/9
port link-mode bridge
port access vlan 30
#interface Ethernet1/0/10 port link-mode bridge
port access vlan 30
#interface Ethernet1/0/11 port link-mode bridge
port access vlan 30
#interface Ethernet1/0/12 port link-mode bridge port access vlan 30
#interface Ethernet1/0/13 port link-mode bridge
port isolate-user-vlan host
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 40 61 untagged
port hybrid pvid vlan 61
#interface Ethernet1/0/14 port link-mode bridge
port isolate-user-vlan host
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 40 62 untagged
port hybrid pvid vlan 62
```

```
# interface Ethernet1/0/15 port link-mode bridge
port isolate-user-vlan host
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 40 63 untagged
port hybrid pvid vlan 63
# interface Ethernet1/0/16 port link-mode bridge
port isolate-user-vlan host
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 40 64 untagged
port hybrid pvid vlan 64
# interface Ethernet1/0/17 port link-mode bridge
# interface Ethernet1/0/18 port link-mode bridge
# interface Ethernet1/0/19 port link-mode bridge
# interface Ethernet1/0/20 port link-mode bridge
# interface Ethernet1/0/21 port link-mode bridge
# interface Ethernet1/0/22 port link-mode bridge
# interface Ethernet1/0/23 port link-mode bridge
port isolate-user-vlan 40 promiscuous
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 10 20 30 40 tagged
port hybrid vlan 61 to 64 untagged
port hybrid pvid vlan 40
# interface Ethernet1/0/24 port link-mode bridge
port isolate-user-vlan 40 promiscuous
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 10 20 30 40 tagged
port hybrid vlan 61 to 64 untagged
port hybrid pvid vlan 40
# interface GigabitEthernet1/0/25 port link-mode bridge
# interface GigabitEthernet1/0/26 port link-mode bridge
# interface GigabitEthernet1/0/27 port link-mode bridge
# interface GigabitEthernet1/0/28 port link-mode bridge
# isolate-user-vlan 40 secondary 61 to 64
# load xml-configuration
# load tr069-configuration
# user-interface aux 0 user-interface vty 0 15
# return
```

5. 交换机 S2 的 display current-configuration 配置信息

```
# version 5.20, Release 2108P01
# sysname S2
# dhcp relay server-group 0 ip 172.0.10.200
# irf mac-address persistent timer irf auto-update enable
undo irf link-delay
```

```
#domain default enable system
#telnet server enable
#ip ttl-expires enable ip unreachables enable
#undo ip http enable
#password-recovery enable
#acl number 2010
rule 0 permit source 172.0.100.0 0.0.0.255
#vlan 1
#
vlan 10
description 研发部
name RD
#vlan 20
description 市场部
name Sales
#vlan 30
description 供应部
name Supply
#vlan 40
description 售后部
name Service
#vlan 61 to 64
#domain system
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
#user-group system
group-attribute allow-guest
#local-user 000000
password cipher $c$3$3KA5a67WH31va89j2BQ09FHhXa9gHR3KHw==
authorization-attribute level 1
service-type telnet local-user admin
password cipher $c$3$QvesFV2XGc1hz/azpK9sxjsP1STBmgCi
authorization-attribute level 3
service-type telnet
#stp region-configuration
region-name H3C
instance 1 vlan 10 20 30 40 61 to 64
active region-configuration
#stp instance 1 root primary
stp enable
#interface Ethernet1/0/3
port link-mode route
ip address 10.0.0.1 255.255.255.252
#interface Ethernet1/0/4
port link-mode route
ip address 10.0.0.5 255.255.255.252
#interface NULL0
```

```
#interface LoopBack0
ip address 9.9.9.202 255.255.255.255
#interface vlan-interface1
ip address dhcp-alloc client-identifier mac vlan-interface1
#interface vlan-interface10
ip address 192.0.10.252 255.255.255.0
undo rip output
vrrp vrid 10 virtual-ip 192.0.10.254
vrrp vrid 10 priority 150
dhcp select relay
dhcp relay server-select 0
#interface vlan-interface20
ip address 192.0.20.252 255.255.255.0
undo rip output
vrrp vrid 20 virtual-ip 192.0.20.254
vrrp vrid 20 priority 150
#interface vlan-interface30
ip address 192.0.30.252 255.255.255.0
undo rip output
vrrp vrid 30 virtual-ip 192.0.30.254
vrrp vrid 30 priority 150
#interface vlan-interface40
ip address 192.0.40.252 255.255.255.0
undo rip output
vrrp vrid 40 virtual-ip 192.0.40.254
vrrp vrid 40 priority 150
#interface Ethernet1/0/1 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40
port trunk pvid vlan 40
#interface Ethernet1/0/2 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40
port trunk pvid vlan 40
#interface Ethernet1/0/5 port link-mode bridge
#interface Ethernet1/0/6 port link-mode bridge
#interface Ethernet1/0/7 port link-mode bridge
#interface Ethernet1/0/8 port link-mode bridge
#interface Ethernet1/0/9 port link-mode bridge
#interface Ethernet1/0/10 port link-mode bridge
#interface Ethernet1/0/11 port link-mode bridge
#interface Ethernet1/0/12 port link-mode bridge
#interface Ethernet1/0/13
port link-mode bridge
#interface Ethernet1/0/14 port link-mode bridge
#interface Ethernet1/0/15 port link-mode bridge
#interface Ethernet1/0/16 port link-mode bridge
```

```
#interface Ethernet1/0/17 port link-mode bridge
#interface Ethernet1/0/18 port link-mode bridge
#interface Ethernet1/0/19 port link-mode bridge
#interface Ethernet1/0/20 port link-mode bridge
#interface Ethernet1/0/21 port link-mode bridge
#interface Ethernet1/0/22 port link-mode bridge
#interface Ethernet1/0/23 port link-mode bridge
#interface Ethernet1/0/24 port link-mode bridge
#interface GigabitEthernet1/0/25 port link-mode bridge
#interface GigabitEthernet1/0/26 port link-mode bridge
#interface GigabitEthernet1/0/27 port link-mode bridge
#interface GigabitEthernet1/0/28 port link-mode bridge
#rip 10
undo summary
version 2
network 10.0.0.0
network 9.0.0.0
network 192.0.10.0
network 192.0.20.0
network 192.0.30.0
network 192.0.40.0
#dhcp enable
load xml-configuration
#load tr069-configuration
#user-interface aux 0 user-interface vty 0 15
acl 2010 inbound
authentication-mode scheme
#return
```

6. 交换机 S3 的 display current-configuration 配置信息

```
#version 5.20, Release 2108P01
#sysname S3
#dhcp relay server-group 0 ip 172.0.10.200
#irf mac-address persistent timer irf auto-update enable
undo irf link-delay
#domain default enable system
#telnet server enable
#ip ttl-expires enable ip unreachables enable
#undo ip http enable
#password-recovery enable
#acl number 2010
rule 0 permit source 172.0.100.0 0.0.0.255
#vlan 1
#vlan 10
description 研发部
name RD
#vlan 20
```

```
description 市场部
name Sales
#vlan 30
description 供应部
name Supply
#vlan 40
description 售后部
name Service
#vlan 61 to 64
#domain system
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
#user-group system
group-attribute allow-guest
#local-user 000000
  password cipher $c$3$j2r3j8wfvFykwYrlWhGFkXfJIIa2gDTnGg==
authorization-attribute level 1
service-type telnet local-user admin
password cipher $c$3$40ds06jOnbzfBDKblQVLoXdHgSWXsLiz
authorization-attribute level 3
service-type telnet
#stp region-configuration
region-name H3C
instance 1 vlan 10 20 30 40 61 to 64
active region-configuration
#stp instance 1 root secondary
stp enable
#interface Ethernet1/0/3
port link-mode route
ip address 10.0.0.2 255.255.255.252
#interface Ethernet1/0/4
port link-mode route
ip address 10.0.0.9 255.255.255.252
#interface NULL0
#interface LoopBack0
ip address 9.9.9.203 255.255.255.255
#interface Vlan-interface1
ip address dhcp-alloc client-identifier mac Vlan-interface1
#interface Vlan-interface10
ip address 192.0.10.253 255.255.255.0
undo rip output
vrrp vrid 10 virtual-ip 192.0.10.254
vrrp vrid 10 priority 120
dhcp select relay
dhcp relay server-select 0
#interface Vlan-interface20
ip address 192.0.20.253 255.255.255.0
```

```
undo rip output
vrrp vrid 20 virtual-ip 192.0.20.254
vrrp vrid 20 priority 120
#interface Vlan-interface30
ip address 192.0.30.253 255.255.255.0
undo rip output
vrrp vrid 30 virtual-ip 192.0.30.254
vrrp vrid 30 priority 120
#interface Vlan-interface40
ip address 192.0.40.253 255.255.255.0
undo rip output
vrrp vrid 40 virtual-ip 192.0.40.254
vrrp vrid 40 priority 120
#interface Ethernet1/0/1 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40
port trunk pvid vlan 40
#interface Ethernet1/0/2 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40
port trunk pvid vlan 40
#interface Ethernet1/0/5 port link-mode bridge
#interface Ethernet1/0/6 port link-mode bridge
#interface Ethernet1/0/7 port link-mode bridge
#interface Ethernet1/0/8 port link-mode bridge
#interface Ethernet1/0/9 port link-mode bridge
#interface Ethernet1/0/10 port link-mode bridge
#interface Ethernet1/0/11 port link-mode bridge
#interface Ethernet1/0/12 port link-mode bridge
#interface Ethernet1/0/13 port link-mode bridge
#interface Ethernet1/0/14 port link-mode bridge
#interface Ethernet1/0/15 port link-mode bridge
#interface Ethernet1/0/16 port link-mode bridge
#interface Ethernet1/0/17 port link-mode bridge
#interface Ethernet1/0/18 port link-mode bridge
#interface Ethernet1/0/19 port link-mode bridge
#interface Ethernet1/0/20 port link-mode bridge
#interface Ethernet1/0/21 port link-mode bridge
#interface Ethernet1/0/22 port link-mode bridge
#interface Ethernet1/0/23 port link-mode bridge
#interface Ethernet1/0/24 port link-mode bridge
#interface GigabitEthernet1/0/25
port link-mode bridge
#interface GigabitEthernet1/0/26 port link-mode bridge
#interface GigabitEthernet1/0/27 port link-mode bridge
#interface GigabitEthernet1/0/28 port link-mode bridge
#rip 10
```

```
undo rip output
vrrp vrid 20 virtual-ip 192.0.20.254
vrrp vrid 20 priority 120
#interface Vlan-interface30
ip address 192.0.30.253 255.255.255.0
undo rip output
vrrp vrid 30 virtual-ip 192.0.30.254
vrrp vrid 30 priority 120
#interface Vlan-interface40
ip address 192.0.40.253 255.255.255.0
undo rip output
vrrp vrid 40 virtual-ip 192.0.40.254
vrrp vrid 40 priority 120
#interface Ethernet1/0/1 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40
port trunk pvid vlan 40
#interface Ethernet1/0/2 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40
port trunk pvid vlan 40
#interface Ethernet1/0/5 port link-mode bridge
#interface Ethernet1/0/6 port link-mode bridge
#interface Ethernet1/0/7 port link-mode bridge
#interface Ethernet1/0/8 port link-mode bridge
#interface Ethernet1/0/9 port link-mode bridge
#interface Ethernet1/0/10 port link-mode bridge
#interface Ethernet1/0/11 port link-mode bridge
#interface Ethernet1/0/12 port link-mode bridge
#interface Ethernet1/0/13 port link-mode bridge
#interface Ethernet1/0/14 port link-mode bridge
#interface Ethernet1/0/15 port link-mode bridge
#interface Ethernet1/0/16 port link-mode bridge
#interface Ethernet1/0/17 port link-mode bridge
#interface Ethernet1/0/18 port link-mode bridge
#interface Ethernet1/0/19 port link-mode bridge
#interface Ethernet1/0/20 port link-mode bridge
#interface Ethernet1/0/21 port link-mode bridge
#interface Ethernet1/0/22 port link-mode bridge
#interface Ethernet1/0/23 port link-mode bridge
#interface Ethernet1/0/24 port link-mode bridge
#interface GigabitEthernet1/0/25
port link-mode bridge
#interface GigabitEthernet1/0/26 port link-mode bridge
#interface GigabitEthernet1/0/27 port link-mode bridge
#interface GigabitEthernet1/0/28 port link-mode bridge
#rip 10
```

```
undo summary
version 2
network 10.0.0.0
network 9.0.0.0
network 192.0.10.0
network 192.0.20.0
network 192.0.30.0
network 192.0.40.0
#dhcp enable
#load xml-configuration
#load tr069-configuration
#user-interface aux 0 user-interface vty 0 15
acl 2010 inbound
authentication-mode scheme
#return
```

7. 交换机 S4 的 display current-configuration 配置信息

```
#version 5.20, Release 1808P12
#sysname S4
#irf mac-address persistent timer irf auto-update enable
undo irf link-delay
#domain default enable system
#telnet server enable
#ip ttl-expires enable ip unreachables enable
#password-recovery enable
#acl number 2010
rule 0 permit source 172.0.100.0 0.0.0.255
#vlan 1
#vlan 10
description 研发部
name RD
#vlan 20
description 市场部
name Sales
#vlan 30
description 供应部
name Supply
#vlan 40
description 售后部
name Service
#vlan 100
#domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#user-group system
 group-attribute allow-guest
```

```
#local-user 000000
password cipher $c$3$7kjfmiVs0QmOWw53RSXXdxptlt92GvEGUg==
authorization-attribute level 1
service-type telnet local-user admin
password cipher $c$3$R2klJ6YNKeSYj9EZxOaL8TH4P9aKDsrc
authorization-attribute level 3
service-type telnet
#interface NULL0
#interface LoopBack0
ip address 9.9.9.204 255.255.255.255
#interface Vlan-interface1
ip address dhcp-alloc client-identifier mac Vlan-interface1
#interface Vlan-interface10
ip address 172.0.10.252 255.255.255.0
vrrp vrid 10 virtual-ip 172.0.10.254
vrrp vrid 10 priority 150
#interface Vlan-interface20
ip address 172.0.20.252 255.255.255.0
vrrp vrid 20 virtual-ip 172.0.20.254
vrrp vrid 20 priority 150
#interface Vlan-interface30
ip address 172.0.30.252 255.255.255.0
vrrp vrid 30 virtual-ip 172.0.30.254
vrrp vrid 30 priority 150
#interface Vlan-interface40
ip address 172.0.40.252 255.255.255.0
vrrp vrid 40 virtual-ip 172.0.40.254
vrrp vrid 40 priority 150
#interface Vlan-interface100
ip address 172.0.100.252 255.255.255.0
vrrp vrid 50 virtual-ip 172.0.100.254
vrrp vrid 50 priority 150
#interface GigabitEthernet1/0/1
port link-mode route
ip address 10.0.0.26 255.255.255.252
ospf timer hello 1
ospf network-type p2p
ospf bfd enable
#interface GigabitEthernet1/0/3
port link-mode route
ip address 10.0.0.33 255.255.255.252
ospf timer hello 1
ospf network-type p2p
ospf bfd enable
#interface GigabitEthernet1/0/2 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
```

```
#interface GigabitEthernet1/0/4 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/5 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/6 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/7 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/8 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/9 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/10 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/11 port link-mode bridge
#interface GigabitEthernet1/0/12 port link-mode bridge
#interface GigabitEthernet1/0/13 port link-mode bridge
#interface GigabitEthernet1/0/14 port link-mode bridge
#interface GigabitEthernet1/0/15 port link-mode bridge
#interface GigabitEthernet1/0/16 port link-mode bridge
#interface GigabitEthernet1/0/17 port link-mode bridge
#interface GigabitEthernet1/0/18 port link-mode bridge
#interface GigabitEthernet1/0/19 port link-mode bridge
#interface GigabitEthernet1/0/20 port link-mode bridge
#interface GigabitEthernet1/0/21 port link-mode bridge
#interface GigabitEthernet1/0/22 port link-mode bridge
#interface GigabitEthernet1/0/23 port link-mode bridge
#interface GigabitEthernet1/0/24 port link-mode bridge
```

```
#interface Ten-GigabitEthernet1/0/25 port link-mode bridge
#interface Ten-GigabitEthernet1/0/26 port link-mode bridge
#interface Ten-GigabitEthernet1/0/27 port link-mode bridge
#interface Ten-GigabitEthernet1/0/28 port link-mode bridge
#ospf 10 router-id 9.9.9.204
silent-interface Vlan-interface10
silent-interface Vlan-interface20
silent-interface Vlan-interface30
silent-interface Vlan-interface40
silent-interface Vlan-interface100
spf-schedule-interval 1
area 0.0.0.0
network 9.9.9.204 0.0.0.0
network 10.0.0.32 0.0.0.3
network 10.0.0.24 0.0.0.3
network 172.0.0.0 0.0.0.255
network 172.0.10.0 0.0.0.255
network 172.0.20.0 0.0.0.255
network 172.0.30.0 0.0.0.255
network 172.0.40.0 0.0.0.255
network 172.0.100.0 0.0.0.255
#ssh client source interface Vlan-interface100
ssh client authentication server 9.9.9.1 assign publickey 9.9.9.1
#telnet client source interface Vlan-interface100
#load xml-configuration
#load tr069-configuration
#user-interface aux 0 user-interface vty 0 15
acl 2010 inbound
authentication-mode scheme
#return
```

8. 交换机 S5 的 display current-configuration 配置信息

```
#version 5.20, Release 1808P12
#sysname S5
#irf mac-address persistent timer irf auto-update enable
undo irf link-delay
#domain default enable system
#telnet server enable
#ip ttl-expires enable
 ip unreachables enable
#password-recovery enable
#acl number 2010
rule 0 permit source 172.0.100.0 0.0.0.255
#vlan 1
#vlan 10
description 研发部
name RD
```

```
#vlan 20
description 市场部
name Sales
#vlan 30
description 供应部
name Supply
#vlan 40
description 售后部
name Service
#vlan 100
#domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#user-group system
 group-attribute allow-guest
#local-user 000000
password cipher $c$3$Z4VEPLQVYpbl+3ohBS664CwO8QKjcVwNrw==
authorization-attribute level 1
service-type telnet local-user admin
password cipher $c$3$yvBMpIg7vUVmCbxAoNWUbi4vpkCDVGjA
authorization-attribute level 3
service-type telnet
#interface NULL0
#interface LoopBack0
ip address 9.9.9.205 255.255.255.255
#interface Vlan-interface1
 ip address dhcp-alloc client-identifier mac Vlan-interface1
#interface Vlan-interface10
ip address 172.0.10.253 255.255.255.0
vrrp vrid 10 virtual-ip 172.0.10.254
vrrp vrid 10 priority 120
#interface Vlan-interface20
ip address 172.0.20.253 255.255.255.0
vrrp vrid 20 virtual-ip 172.0.20.254
vrrp vrid 20 priority 120
#interface Vlan-interface30
ip address 172.0.30.253 255.255.255.0
vrrp vrid 30 virtual-ip 172.0.30.254
vrrp vrid 30 priority 120
#interface Vlan-interface40
ip address 172.0.40.253 255.255.255.0
vrrp vrid 40 virtual-ip 172.0.40.254
vrrp vrid 40 priority 120
#interface Vlan-interface100
ip address 172.0.100.253 255.255.255.0
```

```
vrrp vrid 50 virtual-ip 172.0.100.254
vrrp vrid 50 priority 120
#interface GigabitEthernet1/0/1
port link-mode route
ip address 10.0.0.30 255.255.255.252
ospf timer hello 1
ospf network-type p2p
ospf bfd enable
#interface GigabitEthernet1/0/3
port link-mode route
ip address 10.0.0.34 255.255.255.252
ospf timer hello 1
ospf network-type p2p
ospf bfd enable
#interface GigabitEthernet1/0/2 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/4 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/5 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/6 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/7 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/8 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/9 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
```

```
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/10 port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30 40 100
port trunk pvid vlan 100
#interface GigabitEthernet1/0/11 port link-mode bridge
#interface GigabitEthernet1/0/12 port link-mode bridge
#interface GigabitEthernet1/0/13 port link-mode bridge
#interface GigabitEthernet1/0/14 port link-mode bridge
#interface GigabitEthernet1/0/15 port link-mode bridge
#interface GigabitEthernet1/0/16 port link-mode bridge
#interface GigabitEthernet1/0/17 port link-mode bridge
#interface GigabitEthernet1/0/18 port link-mode bridge
#interface GigabitEthernet1/0/19 port link-mode bridge
#interface GigabitEthernet1/0/20
port link-mode bridge
#interface GigabitEthernet1/0/21 port link-mode bridge
#interface GigabitEthernet1/0/22 port link-mode bridge
#interface GigabitEthernet1/0/23 port link-mode bridge
#interface GigabitEthernet1/0/24 port link-mode bridge
#interface Ten-GigabitEthernet1/0/25 port link-mode bridge
#interface Ten-GigabitEthernet1/0/26 port link-mode bridge
#interface Ten-GigabitEthernet1/0/27 port link-mode bridge
#interface Ten-GigabitEthernet1/0/28 port link-mode bridge

#ospf 10 router-id 9.9.9.205
silent-interface Vlan-interface10
silent-interface Vlan-interface20
silent-interface Vlan-interface30
silent-interface Vlan-interface40
silent-interface Vlan-interface100
spf-schedule-interval 1
area 0.0.0.0
network 10.0.0.32 0.0.0.3
network 10.0.0.28 0.0.0.3
network 9.9.9.205 0.0.0.0
network 172.0.0.0 0.0.0.255
network 172.0.10.0 0.0.0.255
network 172.0.20.0 0.0.0.255
network 172.0.30.0 0.0.0.255
network 172.0.40.0 0.0.0.255
network 172.0.100.0 0.0.0.255
#load xml-configuration
#load tr069-configuration
#user-interface aux 0 user-interface vty 0 15
```

```
acl 2010 inbound
authentication-mode scheme
# return
```

```
acl 2010 inbound
authentication-mode scheme
# return
```

参 考 资 料

[1] H3C 认证网络工程师(H3CNE):构建中小企业网络实验指导书
[2] H3C 认证网络工程师(H3CNE):构建中小企业网络学习指导书(上册)
[3] H3C 认证网络工程师(H3CNE):构建中小企业网络学习指导书(下册)
[4] H3C 认证路由交换网络高级工程师(H3CSE-Routing & Switching):构建 H3C 高性能园区网络学习指导书(上册)
[5] H3C 认证路由交换网络高级工程师(H3CSE-Routing & Switching):构建 H3C 高性能园区网络学习指导书(下册)
[6] H3C 认证路由交换网络高级工程师(H3CSE-Routing & Switching):H3C 大规模网络路由技术实验指导书
[7] H3C 网络学院教程:中小企业网络应用案例
[8] H3C 网络学院教程:H3C SDN 实验课程教材
[9] 杭州华三通信技术有限公司.路由交换技术[M]. 3 卷.北京:清华大学出版社,2012.
[10] 2017 年福建省职业院校技能大赛计算机网络应用赛项模拟试题
[11] 2016 年福建省职业院校技能大赛计算机网络应用赛项模拟试题
[12] 2016 年全国职业技能大赛高职组计算机网络应用赛项赛题题库 10 套题
[13] 2016 年全国职业技能大赛高职组计算机网络应用赛项(正式考题)——C 套及答案